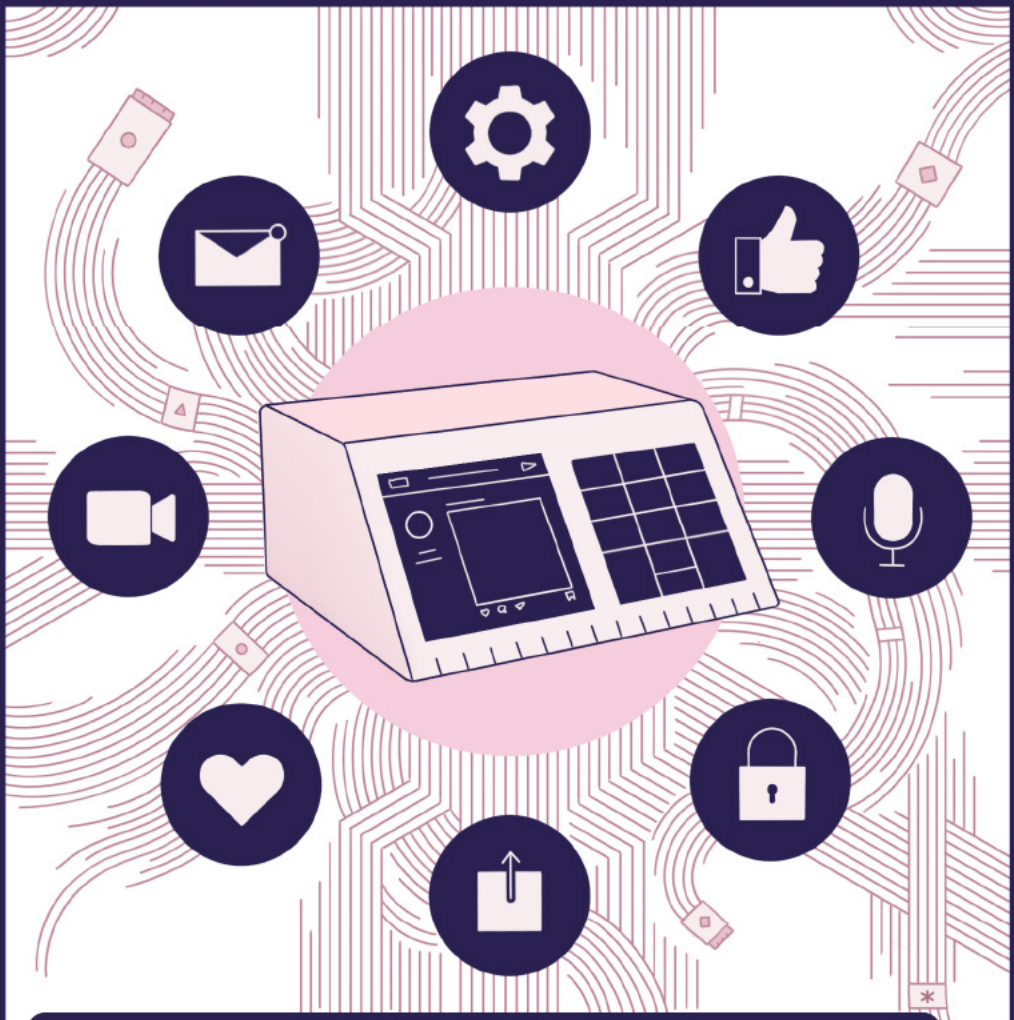


ELEIÇÕES E INTERNET

guia para proteção de direitos nas campanhas eleitorais

COALIZÃO DIREITOS NA REDE

FICHA TÉCNICA

INTERNET E ELEIÇÕES
Guia para proteção de direitos nas campanhas eleitorais

Cartilha realizada com base em documentos de trabalho do GT de Eleições da Coalizão Direitos na Rede e em materiais de oficinas da Rede Transfeminista de Cuidados Digitais para orientar candidaturas em suas campanhas na Internet.

Autoras
Ladyane Souza (#MeRepresenta)
Joana Varon (Coding Rights)

Assistente Editorial
Thayná Yaredy (#MeRepresenta)

Revisão
Evorah Cardoso (#MeRepresenta)
Violeta
Olívia Bandeira, Bia Barbosa e Maria Mello (Intervozes)

Ilustração e Diagramação
Clarote (Coding Rights)

Pesquisadores dos documentos de trabalho do GT de Eleições
Violência Política e de Gênero: Evorah Cardoso, Joana Varon e Maria Luiza Freire Mercês
Proteção de Dados: Francisco Brito Cruz e Heloisa Massaro
Desinformação: Olívia Bandeira e Maria Mello

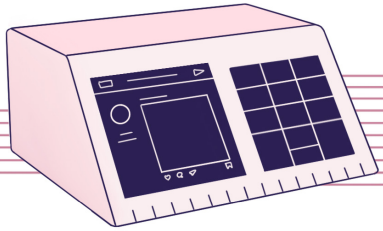
Uma iniciativa da

COALIZÃO DIREITOS NA REDE

Execução

CODING RIGHTS

#ME REPRESENTA



Força Tarefa Internet e Eleições
Amarc Brasil - Taís Ladeira
Casa de Cultura Digital de Porto Alegre - Janaína Spode
Coding Rights - Joana Varon
InternetLab - Francisco Brito Cruz
Internet Sem Fronteiras - Josué Gomes
Intervozes - Bia Barbosa, Flávia Lefèvre, Maria Mello e Olivia Bandeira
Instituto de Referência em Internet e Sociedade (IRIS) - Gustavo Ramos Rodrigues
IP.Rec - Mariana Canto e Raquel Saraiva
#MeRepresenta - Evorah Cardoso e Maria Luiza Freire Mercês
Bruna Martins

Secretaria Executiva
Fabrício Solagna

Comunicação
Ênio Lourenço

Assessoria de imprensa
Adriana Veloso

Apoio
Fundação Ford e Hivos

Agradecimentos
Rede Transfeminista de Cuidados Digitais, Mariana Valente e Samara Costa

Licença Creative Commons Non Commercial Share Alike

Data de publicação: Setembro, 2020

ÍNDICE

APRESENTAÇÃO DA CARTILHA 06

O QUE PODE E O QUE NÃO PODE DURANTE A E-CAMPANHA? 08
Checklist 08
Recursos da Campanha 10

QUAIS OS DESAFIOS DE UMA CAMPANHA ELEITORAL DIGITAL? 12
Acesso à Internet de candidaturas e eleitorado 12
Violência política digital e suas interseccionalidades 16
Ataques mais frequentes 19
Discurso de ódio 20
"Fake News" e desinformação 23
Proteção de dados pessoais e privacidade 27

PODEMOS USAR AS TECNOLOGIAS PARA NOS PREVENIR DE ATAQUES? 31
Modelo de ameaças 31
Dicas básicas de cuidados digitais preventivos 34
Senhas fortes por todos os lados 34
Autenticação de dois fatores para evitar roubo de contas 35
Criptografia para proteger comunicações e armazenar dados 36
Configurações de privacidade e segurança: estamos compartilhando mais informações do que é preciso? Qual nosso rastro digital? 38
Gestão de identidades: em uma, já somos muitas 40
Cuidado no click! Malware e vírus 42
Sistemas atualizados e backups seguros 43
Prepare-se em caso de perda de celular 43
Zoombombing: ataque em videoconferências 43
Guias bastante acessíveis com dicas de segurança 46

O QUE FAZER EM CASO DE ATAQUES? 47
Medidas de segurança digital para mitigação de danos 48
Denúncias nas plataformas 49
Documentação sobre o ataque 49
Denúncias no Judiciário 50
O que diz a legislação? 50
Marco Civil da Internet 51
Lei Geral de Proteção de Dados Pessoais (LGPD) 53
Legislação Eleitoral e propaganda irregular 55
Direito de Resposta - Lei nº 13.188/2015 56
Código Eleitoral - Lei nº 4.737/1965 56
Lei Eleitoral - Lei nº 9.504/1997 57
Resolução nº 23.610/2019 58
Legislação Penal 58
Código Penal de 1940 58
Lei Antirracista - Lei nº 7.716/1989 60
Lei das Contravenções Penais - Decreto-lei nº 3.688/1941 61
Combate à Violência de gênero na Internet 62
Lei Carolina Dieckmann - Lei nº 12.737/2012 62
Lei Lola - Lei nº 13.642/2018 62
Lei Maria da Penha - Lei nº 11340/2006 63
Criminalização da LGBTfobia - STF ADO 26 e MI 4733 63
Canais de denúncia e possibilidades de enfrentamento: Respostas efetivas a ataques na Internet 64
Redes de apoio 66

FORTALECIMENTO DO ESPAÇO DEMOCRÁTICO DA INTERNET 67

REFERÊNCIAS DA CARTILHA 68

LINKS ÚTEIS 71

APRESENTAÇÃO DA CARTILHA

Esta cartilha foi idealizada para ser um material de consulta fácil e acessível, com orientações a candidaturas sobre direitos na Internet para as eleições municipais de 2020.

Fazer uma eleição no contexto de pandemia torna a Internet ainda mais central para a disseminação de informações seguras e confiáveis aos eleitores dos mais de cinco mil municípios, ao mesmo tempo em que traz uma série de desafios para as candidaturas, partidos, eleitores, atores do sistema de justiça eleitoral e, também, para o setor privado – em especial, para grandes plataformas digitais que detêm o monopólio das redes sociais, como Facebook, Whatsapp, Google, Twitter e Instagram.

Mais do que nunca, as eleições estarão sob influência dos debates digitais para a formação da chamada ***opinião pública***, justificando a preocupação da sociedade civil, como as entidades que compõem a **Coalizão Direitos na Rede**, com a proteção de dados de eleitores, riscos a sua autonomia para se informar e decidir seu voto, bem como a possibilidade de ataques virtuais e ameaças à privacidade de candidaturas. Escândalos como o da Cambridge Analytica e Facebook mostram que nossos dados pessoais na Internet podem ser utilizados de forma abusiva para conhecer melhor determinado grupo de eleitores, encaminhar mensagens distintas direcionadas a cada grupo para ter maior poder de persuasão e até de manipulação sobre esse eleitorado, promovendo ataques a adversários políticos.

Destacamos alguns exemplos de desafios à cidadania e à formação da opinião pública nas eleições de 2020:

- A possibilidade de ***direcionamento e microdirecionamento*** pode favorecer divisões no eleitorado e no debate público, além de reduzir a transparência sobre a totalidade das campanhas, diante da possibilidade de que

mensagens contraditórias sejam veiculadas paralelamente a públicos distintos.

- A questão de ***monetização*** de conteúdos também gera novos problemas: ganha-se dinheiro a partir dos ***views e likes***, mas como tal valor poderá ser declarado ou mesmo fiscalizado nas campanhas de 2020?

- A promoção deliberada de ***desinformação*** - as chamadas ***fake news*** -, a disseminação de discurso de ódio, de ataques, ameaças e até mesmo o sequestro de dados como ferramentas para ganhar votos constituem práticas de ***violência política,*** um conceito que explicaremos detalhadamente em seu aspecto multidimensional.

Todas são preocupações com a democracia: de um lado, proteger o processo eleitoral, coibindo práticas violentas e, de outro, garantir sua diversidade, sem ferir os direitos à informação e à liberdade de expressão dos usuários das redes sociais. A pressão por respostas fez com que uma série de medidas venha sendo adotada pelas plataformas e pela Justiça eleitoral, algo que vamos contar a vocês nas páginas seguintes.

Deve ser compromisso de toda a sociedade o exercício da cidadania também na Internet. Acreditamos que o compromisso com a pluralidade política e com a garantia de direitos e liberdades no espaço digital é um passo importante, embora outros desafios permaneçam, como: a campanha digital poderá se democratizar e atingir, por exemplo, o voto do eleitorado periférico, da população rural ou indígena?

Aqui pretendemos construir pontes nesse debate, fornecer informações a candidaturas sobre direitos em espaços virtuais, explicar o funcionamento de alguns ***canais de denúncia***, bem como trazer cuidados de segurança, num esforço de dar algumas pistas de como podemos fazer acontecer nossa ***democracia em rede.***

O QUE PODE E O QUE NÃO PODE DURANTE A E-CAMPANHA?

Tentamos reunir algumas informações em um ***checklist*** para te ajudar:

Não pode

- **Doações de empresas a candidaturas** (não pode doar banco de dados também)
- **Disparo em massa de conteúdo**, sem anuência do destinatário
- **Venda de cadastros** de endereços eletrônicos
- **Livemício** (show na Live)
- **Impulsionamento e disseminação de conteúdo falso** *(fake news)*
- **Propaganda em sites** de empresas ou sites oficiais do poder público
- **Discurso de ódio** (ofensa à honra ou imagem de candidato, partido político ou coligação)
- **Perfis falsos**
- **Propaganda paga,** exceto impulsionamento nas redes sociais
- **Impulsionamento de publicação** que veicule propaganda negativa de outras candidaturas, ou mesmo edição de vídeo ou áudio para prejudicar outro candidato, partido político, coligação (isso também vale para eleitores e apoiadores)

Pode

- Artista conversando na Live, **sem fazer shows ou apresentações artísticas**
- **Site do candidato**, desde que seja hospedado no Brasil (.br) e comunicado à Justiça Eleitoral no registro da candidatura
- **Coleta de dados cadastrais durante atividades eleitorais**, informando eleitores sobre finalidade. Ex. "se quiser receber informações da campanha, deixe aqui seus dados para cadastro"

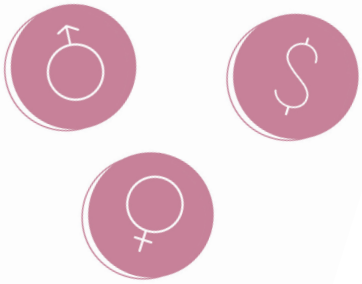
  neste caso, é permitido apenas usar o banco de dados que você construiu para você, ou que o seu partido ou coligação construíram

  você deve oferecer opção de descadastramento, caso a pessoa não queira mais receber informações, retirando-a em até 48h do cadastro e não enviando mais conteúdos
- **Propaganda eleitoral na Internet** por meio de blogs, redes sociais, sítios de mensagens instantâneas e aplicações de Internet assemelhadas, dentre as quais aplicativos de mensagens instantâneas, desde que os contatos tenham sido cadastrados gratuitamente pelos candidatos, partidos ou coligações
- **Impulsionamento pago de conteúdo eleitoral** nas redes sociais, mas para isso ele deve vir identificado como propaganda eleitoral e trazer o CNPJ ou CPF da pessoa responsável - isso vale tanto para candidaturas quanto para apoiadores
- **Financiamento coletivo** por vaquinha virtual apenas em ***plataformas cadastradas no Tribunal Superior Eleitoral (TSE)***

Recursos da campanha

A distribuição do total recebido do Fundo Especial de Financiamento de Campanha (FEFC) pelo partido deve ser realizada de modo proporcional ao número de candidaturas de cada gênero inscritas no partido, sendo garantido um mínimo 30% de candidaturas para qualquer dos gêneros. Na prática, isso significa condições mínimas para candidaturas de mulheres, pois hoje temos apenas 13,5% de mulheres vereadoras e 13,93% prefeitas. A decisão recente do Tribunal Superior Eleitoral sobre a necessidade de financiamento proporcional também para candidaturas de pessoas negras só valerá para as eleições de 2022.

É importante conferir no site ***divulgacand.br*** o montante que o partido declarou que você recebeu e o quanto você de fato recebeu, além de outras ferramentas e estatísticas que o site disponibiliza, pois isso pode ajudar candidatas mulheres a não serem usadas pelos partidos apenas para cumprir cota ou para desvio de seus recursos de campanha para outras candidaturas. Além disso, pode haver o financiamento coletivo, as conhecidas vaquinhas, uma modalidade de captação de recursos para campanhas criada pela ***Lei nº 13.488/2017***. Sua modalidade virtual deve ser realizada a partir de um **site confiável** e cadastrado no Tribunal Superior Eleitoral (***verifique aqui***). É importante ainda comparar os custos das taxas de administração de cada uma delas, que variam significativamente.



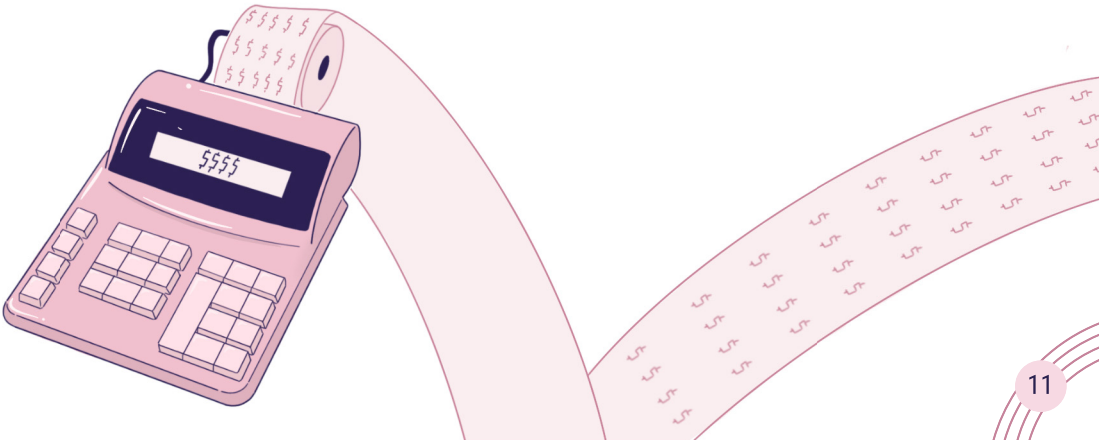
Cuidados e atenção na prestação de contas eletrônica

Como fazer?

A prestação de contas da campanha deve ser feita através do programa desenvolvido pela Justiça Eleitoral, o **Sistema de Prestação de Contas Eleitorais** ***(SPCE)***, um aplicativo a ser instalado no computador para que as candidaturas possam preencher informações relativas às despesas eleitorais.

Prazos

Os relatórios financeiros de campanha devem ser enviados pelo SPCE até 72h após o recebimento de cada uma das doações; as prestações de contas **parciais** de todas as candidaturas ocorrem de 21 a 25.10.2020 e as **finais**, ou seja, para candidaturas à Prefeitura que forem disputar o segundo turno, ocorrem até 15.12.2020.

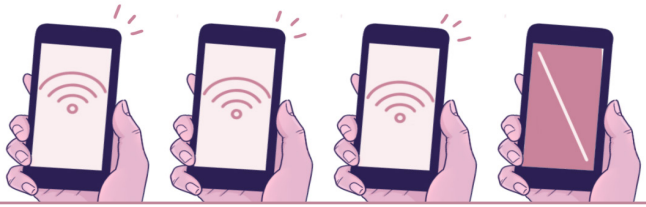


QUAIS OS DESAFIOS DE UMA CAMPANHA ELEITORAL DIGITAL?

Acesso à Internet de candidaturas e eleitorado

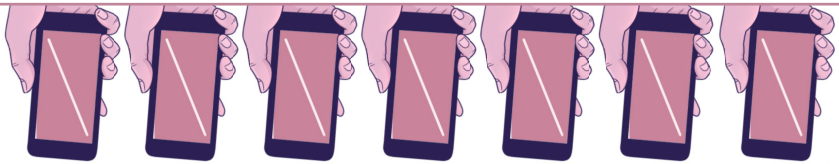
Quando pensamos em campanha política, uma das primeiras coisas que nos vêm à cabeça são palanques, praças cheias, eventos e distribuição de panfletos, bandeiras, santinhos, carro de som e megafone. O que fazer agora que as ruas precisam ser - mais do que já vinham sendo - substituídas pelas plataformas digitais, por uma questão de saúde pública? Quem se lança na corrida eleitoral precisará se adaptar à linguagem virtual, e um primeiro passo é entender quem tem acesso a ela.

O Brasil é um país muito desigual e isso também se reflete no acesso à tecnologia, equipamentos e à Internet, o que por sua vez pode replicar e amplificar desigualdades, opressões e violências do campo social, como a discriminação racial e de gênero, além de consolidar ou favorecer elites políticas. Apesar disso, defendemos que a tecnologia tem a potencialidade de ser uma ferramenta de inclusão, principalmente quando as pessoas têm mais informações sobre como utilizá-la e sobre seus direitos. Entender melhor as ferramentas de informação, participar em fóruns de debate e expressão política são **chaves de mudança;** saber aproveitá-las e ampliar o acesso a elas pode contribuir para uma maior representação de grupos minorizados no debate público.

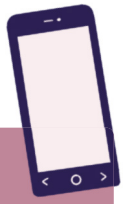


1 em cada 4 brasileiros não utiliza a Internet

47 milhões de pessoas não possuem acesso à Internet



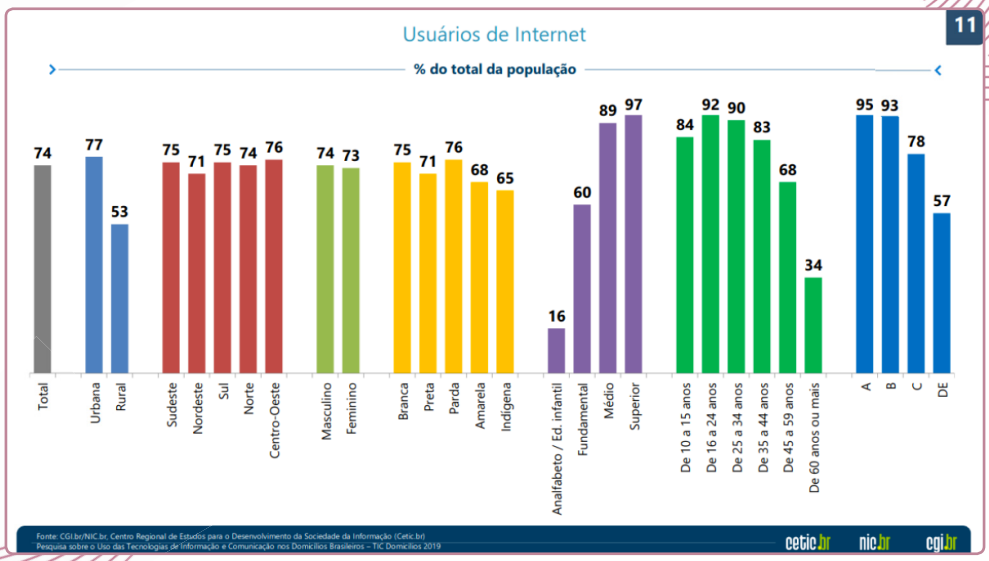
58% acessa a internet somente pela celular



Na área rural, **o celular representa 79% dos acesso**

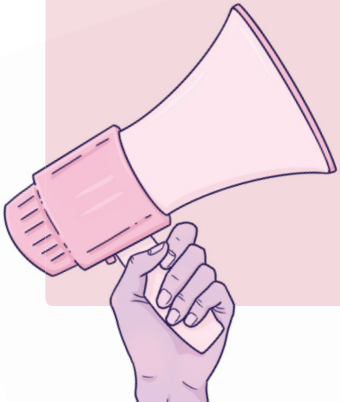
Nas classes DE o **uso exclusivo pelo celular chega à 85%**

dados do TIC domicílios 2019 - Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br)



Garantia do direito do acesso à Internet a todos

Está definida no Marco Civil da Internet (Lei nº. 12.965/2015), em seu artigo 4º. Quando pensamos esse direito como ferramenta essencial ao exercício da democracia, no caso das eleições, se torna ainda mais relevante defendê-lo e ampliá-lo. Na legislação nacional, a Lei Geral de Telecomunicações também dá subsídio a esta linha de pensamento, ao determinar que serviços de telecomunicações considerados essenciais, como a banda larga, não possam ser prestados unicamente em regime privado, mas devam ser também explorados em regime público, com metas de universalização. Ou seja, o acesso deve ser para todos, em prol do interesse público e como instrumento de concretização de políticas públicas. A realidade brasileira hoje é muito desigual, de maneira que a concretização do direito de todos à Internet se torna um ideal a ser perseguido.



Ante tamanha desigualdade, candidatas/es/os devem diversificar as plataformas que utilizam na campanha, inclusive para além da Internet, com divulgação em TV e rádio, se quiserem alcançar um número maior de eleitores. Considerando a maior parte dessa conexão se dá via **smartphones**, uma boa estratégia é investir em conteúdos que possam ser acessados pelo celular e que não precisem de muito consumo de dados, sem precisar fazer *download*.

A diversidade de estratégias de campanha pode variar em cada plataforma, mas desafios comuns a todas são a falta de contato que uma campanha presencial permite - com gestos, olhares e expressões faciais, - a dificuldade na organização da participação e engajamento dos eleitores, a realização de eventos, o excesso de informação, a disputa por atenção e, por fim, a produção de conteúdo.

Se você tiver condições financeiras, é importante ter uma pessoa dedicada para a comunicação nas redes, que possa te ajudar a manter uma frequência digital e a produzir conteúdo direto, coerente, com *#Hashtags* e estratégias, como o chamado *storytelling* - que nada mais é do que contar histórias que te conectem com seu eleitorado. Ter contato com alguém que entenda sobre **impulsionamento, alcance e engajamento** em redes sociais também pode ser um diferencial para manter uma comunicação com seus eleitores e para que você possa aumentar sua conectividade e transmitir sua mensagem por meio das plataformas. Para isso, também é importante saber o perfil do eleitorado na sua cidade, que você pode consultar ***aqui***.

Perfil do Eleitorado - TSE 2020

homens 47,48%

mulheres 52,49%

25,47% concluíram o **Ensino Médio**

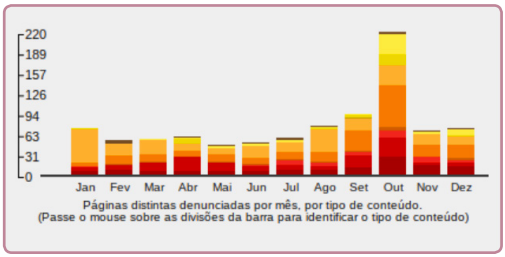
0,68% concluíram o **ensino superior**

Violência política digital e suas interseccionalidades

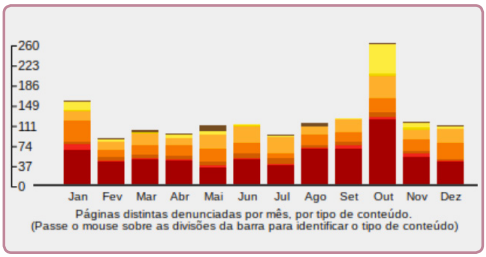
Acreditamos que a Internet pode ser uma ferramenta para amplificar a voz de grupos marginalizados. No entanto, o mundo digital também se tornou muitas vezes um fórum de desinformação, incitação ao ódio, assédio e outras formas de ataques. Segundo dados da ONG SaferNet (***indicadores***), o contexto eleitoral está relacionado a uma explosão de denúncias de racismo, xenofobia, apologia e incitação a crimes contra a vida na Internet. Verificamos que há, em verdade, um **contínuo** de violência, em que cybercrimes estão relacionados a crimes e desigualdades do cotidiano fora das redes, e que a Internet pode amplificar determinada realidade e viralizar tentativas de silenciamento de candidaturas, transformando-a em um campo de batalha durante as campanhas eleitorais.

Eleições são um contexto de aumento da violência a direitos na Internet.

2014



2018



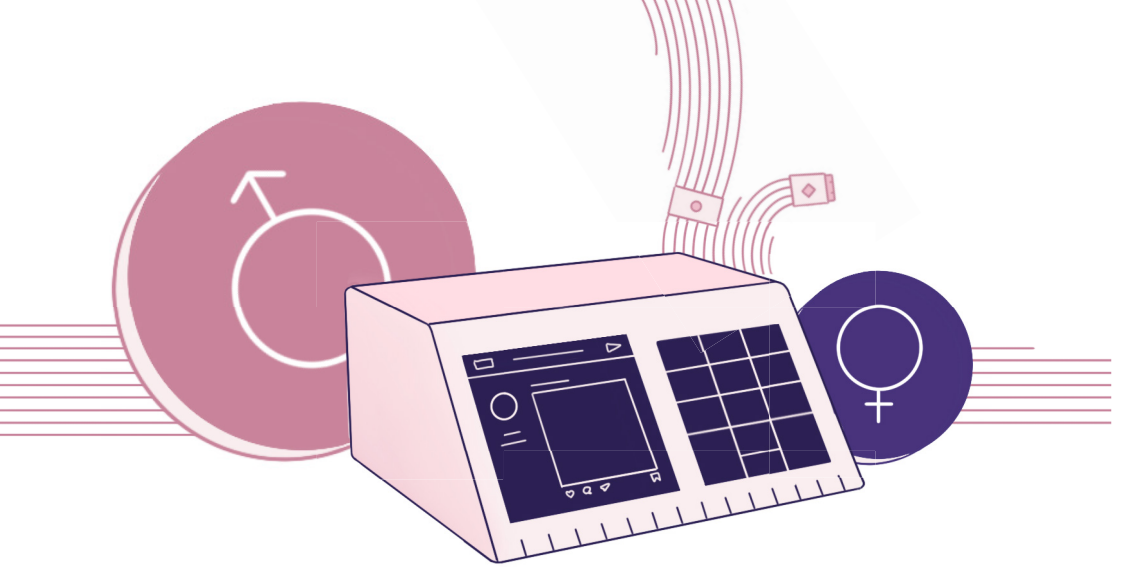
obs.: aumento expressivo de casos de violência na Internet nos meses de outubro dos anos de eleições para governador, presidente, deputado distrital, estadual, federal e senador.

Violência Política: o que é?

Violência direcionada a candidaturas, que pode ser praticada on ou offline, destinada a atingir candidatas/es/os, prejudicando ou influenciando o processo eleitoral em relação à representatividade e democracia. Se inicia no período de campanhas políticas e continua no exercício dos mandatos, dificultando a manutenção no poder. Tal violência engloba todas as manifestações agressivas que buscam minar a cidadania e voz das candidaturas, intimidando desde pequenos comentários até ameaças e violências físicas, que podem fazer com que mulheres, pessoas negras e LGBTQIA+ se autocensurem, permaneçam em silêncio ou se retirem da política.

Quem é mais afetado?

As candidaturas mais afetadas são aquelas que historicamente foram privadas de exercer seus direitos políticos, e assim não tiveram esse lugar da política como "dado" ou "natural"; ou seja, se você é candidata/o/e e não se define como homem, ou como pessoa branca, heterossexual e cisgênero, provavelmente você já sofreu as violências categorizadas nesta cartilha. Reforçamos que essas violências não existem de maneira isolada, mas sim coexistem e se reforçam, em uma opressão interseccional ou multidimensionalidade de opressões (Moreira, 2017, p. 115). Desde sempre os grupos vulnerabilizados têm sofrido violência em razão de sua raça, gênero, orientação afetivo-sexual, sobretudo quando se candidatam à política, e agora esses candidatos/as/es também devem enfrentar esse discurso nas campanhas digitais.



A violência política de gênero é um fenômeno que vem sendo documentado no Brasil e no mundo. Em uma pesquisa com mais de 300 prefeitas eleitas nas últimas eleições de 2016 ("***Perfil das Prefeitas no Brasil: mandato 2017-2020" - Instituto Alziras, 2018***), 53% delas afirmaram ter sofrido assédio ou violência política pelo simples fato de serem mulheres. As prefeitas mais jovens percebem mais os casos de violência (91% das com menos de 30 anos) do que as mais velhas (40% das prefeitas entre 50 e 60 anos e apenas 27% das acima de 60 anos). Ainda assim, vivemos um contexto em que mulheres na política não estão mais naturalizando essas formas de violência como sendo parte do jogo.

A **violência política** praticada na **Internet ou por meio da tecnologia** para silenciar vozes e cercear liberdades tem algumas características próprias do uso da rede. Estudos de mapeamento de formas de violências de gênero no ambiente online ("***Violências de gênero na Internet: diagnóstico, soluções e desafios***" com mapa dinâmico ***aqui*** - Coding Rights; InternetLab, 2017 e "***Consentimento: nossos corpos como dados***" - Peña; Varon, 2019) identificaram situações específicas de violência política na Internet. Entendemos que nomear a **violência política na Internet** é um primeiro passo contra a sua normalização e banalização.

Ataques mais frequentes

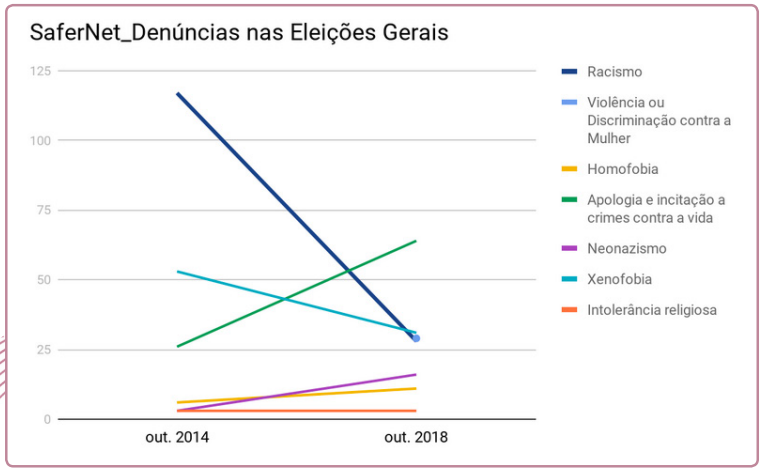
Desinformação	Campanhas de desprestígio (que visam o descrédito da pessoa atacada) Difusão de informação falsa (muitas vezes ligada a sexualidade e casamento)
Violações de privacidade	Exposição de dados pessoais (doxxing) Vazamento de dados pessoais, privados e de orientação sexual compilados sem consentimento ou com consentimento por um clique Compartilhamento não consentido de imagens íntimas (exposição de intimidade) Utilização não consentida de materiais e fotos Roubo de identidade
Ofensas	Discurso de ódio Cyber Bullying/ofensa Exploração sexual e estereotipada da imagem Edição de imagens e vídeos
Ameaças	Assédio sexual e moral Assédio via inbox nas redes sociais, com fotos e vídeos obscenos Stalking Ameaças de violência física
Censura	Ataque massivo e coordenado Manipulação de algoritmos Remoção de conteúdo Bloqueio de posts, páginas e perfis por denúncia ou iniciativa das redes sociais
Invasões	"Zoombombing" (invasão de videoconferência ou evento online) Acesso não autorizado a contas ou dispositivos pessoais Invasão/Ataques à segurança de sistemas

A relação e a interconexão entre essas violências configuram a **violência política de gênero na Internet**. A partir deste cenário, sugerimos que as candidatas/es/os entendam um pouco em que contextos se dão esses ataques.

Discurso de ódio

Uma das principais formas de violência política é o **discurso de ódio**. No Brasil os discursos de ódio mais frequentes geralmente são discriminatórios em relação à identidade e expressão de gênero, raça, etnia, religião, orientação afetiva e sexual, origem social, origem geográfica/xenofobia (nordestino, estrangeiro), pertencimento a um grupo cultural, ideológico-político ou não (feminista, comunista), estados de saúde física ou mental, deficiência.

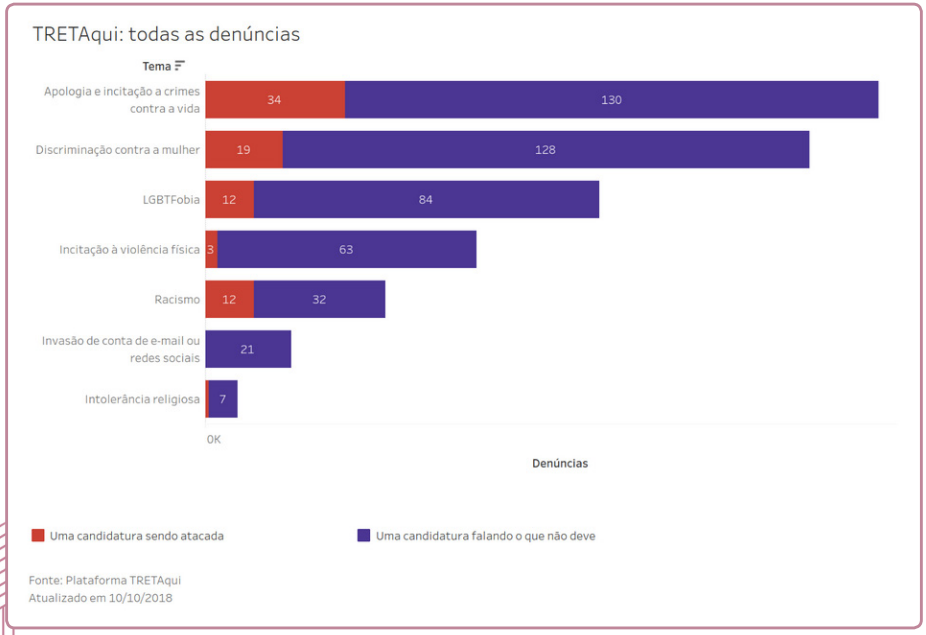
A Internet possibilitou uma velocidade nunca antes vista na replicação de informações, o que faz com que as redes sociais se tornem muitas vezes catalisadoras de discurso de ódio, viralizando publicações deste tipo. Usuários das redes acabam sendo replicadores desses conteúdos ao curtir, salvar, compartilhar, já que a lógica dos algoritmos das redes sociais amplia a visibilidade de conteúdos que têm mais interação. Comumente os picos de denúncias de discurso de ódio estão relacionados a eventos fora da Internet, como manifestações, ou nas eleições.



Elaboração própria a partir de indicadores de denúncias da SaferNet

Vale reforçar que o **discurso de ódio contra candidaturas** é um ato de violência cuja utilização em contextos eleitorais tem o objetivo exclusivo de silenciar a expressão de candidaturas representativas de grupos minoritários. Ele causa um acirramento do debate político e polarização no país, além de fomentar a violência dentro e fora dos pleitos eleitorais. Já o **discurso de ódio praticado por candidaturas** revela sua instrumentalização como ferramenta de marketing político eleitoral, adotada não apenas por campanhas isoladamente, mas também por partidos, valendo-se, principalmente, das redes sociais para sua propagação.

Nas eleições de 2018, a plataforma ***TretAqui.org*** recebeu 564 denúncias de links, principalmente de candidaturas que estavam atacando outras candidaturas e grupos da população com manifestações misóginas, LGBTfóbicas e racistas:



Tais comportamentos, quando realizados em plataformas digitais, como Twitter, Facebook, Youtube, Instagram, encontram algumas barreiras nos próprios **Termos de Uso e Padrões da comunidade destas plataformas**. Todavia, não são encontrados muitos dados sobre como ocorre a remoção de conteúdos denunciados nessas plataformas, que também são responsáveis por ampliar sua disseminação ao premiar interações, mesmo que automatizadas. Quantos e quais conteúdos são removidos por meio de denúncias nessas plataformas? Quais são removidos por meio de filtros no algoritmos? Mais transparência sobre como essas empresas lidam com esses ataques nos daria ferramentas mais consistentes, inclusive para o Judiciário atuar no combate a condutas violentas.

Eleições 2018

Dados da SAFERNET obtidos durante as eleições de 2018 mostram que durante os 21 dias do 1º ao 2º turno as denúncias com teor de xenofobia, apologia e incitação a crimes contra a vida, neonazismo, homofobia, racismo e intolerância religiosa cresceram bastante: o número total de denúncias mais que dobrou em relação ao pleito de 2014, ou seja, passou de 14.653 para 39.316 em 2018. A maior parte do conteúdo denunciado se trata de violência cometida no Facebook (13.592 denúncias) em segundo lugar vem o Twitter (1.509), seguido de Instagram (1.088) e do YouTube (400).

Importante ressaltar que o **discurso de ódio** proferido na Internet durante as eleições **transcende o ambiente digital**. Estudo da Gênero e Número (***Violência contra LGBT+ nos contextos eleitoral e pós-eleitoral, 2019***), entrevistando pessoas LGBTQIA+ de diferentes cidades, revelou que "51% dos entrevistados sofreram pelo menos uma agressão durante o segundo semestre de 2018 e 87% relatam ter tomado conhecimento de violências cometidas contra conhecido/a LGBT+ ou pessoa próxima LGBT+ no mesmo período". Novamente, mulheres são as maiores vítimas. De acordo com a pesquisa, "as mulheres lésbicas foram um dos grupos que mais declararam ter sofrido violência (57%), seguidas das pessoas trans e travestis (56%), gays (49%) e pessoas bissexuais (44,5%)."

Relacionadas ao **discurso de ódio,** identificamos a prática de outras violências, como a promoção de informações falsas e a divulgação e uso dados pessoais sem consentimento, violências articuladas com o intuito de impor um discurso de medo e perigo, intencionalmente silenciador e intimidador.

"Fake news" e desinformação

Desinformação, "fake news", notícia falsa, mentira... cada vez mais escutamos esses termos sem muita clareza sobre o que é o que. Nessa cartilha, ainda que as chamadas "fake news" tenham se popularizando como denominação, optamos por tratar do assunto a partir do conceito de **desinformação**, aqui entendido como uma forma deliberada de disseminação de informação enganosa com o objetivo de atingir determinado fim.

No dia-a-dia da população brasileira, as redes sociais e o WhatsApp são utilizadas como fonte de informação dominante, o que pode ser decisivo para as eleições. Isto posto, o problema da disseminação de notícias falsas ganha proporção cada vez maior no país.

Não se trata de qualquer mentira. Muitas vezes são conteúdos que viralizam nas redes sociais simulando uma **notícia**, com **estilo jornalístico**, mas divulgando informações comprovadamente falsas,

muitas vezes utilizando-se também de discursos de ódio e até mesmo ocultando autoria. Não se trata de uma opinião, em que você pode discordar ou concordar, mas de uma desinformação, mascarada de notícia.

Em muitos casos a disseminação da desinformação se dá por empresas contratadas, que se utilizam de contas automatizadas (ou bots), redes organizadas e grupos de WhatsApp para garantir ampla disseminação das notícias falsas. As campanhas de 2020 vão ocorrer também nesse contexto em que, infelizmente, candidaturas terão que lidar com essas verdadeiras "máquinas" da **mentira e de desinformação.**

A questão fica ainda mais complicada se considerarmos que algumas plataformas digitais, ao monetizarem o tráfego elevado de usuários, também podem acabar lucrando e gerando lucro para quem dissemina desinformação polarizando o debate e propositalmente confundindo o eleitorado.

Ainda que não seja possível medir concretamente o quanto uma notícia falsa divulgada impacta o voto, por enquanto, há diversas ações que podem ser adotadas para combater essa tendência. Entre elas:

Repassar essas informações para checadores de fatos;

Denunciar as publicações com conteúdo falso e os perfis falsos criados para disseminá-las nas próprias plataformas;

Propagar o argumento verdadeiro;

Fomentar leitura crítica de mídia como exercício responsável de cidadania;

Cobrar transparência das plataformas de Internet, tanto sobre a receita com anúncios e o alcance desse tipo de publicações quanto sobre a remoção de perfis automatizados criados com a finalidade de propagar desinformação;

Denunciar práticas e campanhas de desinformação à Justiça e ao Ministério Público Eleitoral.

Do ponto de vista das campanhas e partidos políticos, é fundamental ainda realizar formações sobre o tema para candidaturas, a partir da ideia de que uma boa forma de combate à desinformação é a produção e disseminação de informação confiável. Assim como incentivar a checagem de informações disseminadas por seus partidários e apoiadores, além de orientá-los sobre o que fazer em caso de identificação de distribuição deliberada de desinformação.

Desconfie // Checagem de fatos

As ações de checagem de conteúdos falsos encontram dificuldades. Além das relacionadas ao volume de informações a ser verificado e ao alcance das checagens, muito menor que o dos conteúdos falsos, há o problema de se definir o que é desinformação e quais informações serão ou não verificadas. De toda maneira, existem agências de checagem gratuitas que podem te ajudar a conferir as notícias e que respondem inclusive por WhatsApp: Aos fatos, Agência Lupa, Fato ou Fake.

Procure também:

Pesquisar os especialistas mencionados na notícia, ver se o fato foi veiculado em mais de um site e em algum site confiável.

Avaliar se o texto contém palavras em letras maiúsculas, erros de digitação e ortografia, exclamações, abreviações, excesso de adjetivos, sensacionalismo e muitas opiniões e pedido de compartilhamento - esses são sinais de alerta.

Denunciar o conteúdo suspeito ou falso no Facebook, Instagram, YouTube, Twitter e até mesmo no WhatsApp (através dos três pontinhos no canto superior direito da tela).

Contas falsas e perfis automatizados para disseminar desinformação

É bastante comum que agressores virtuais utilizem perfis falsos e/ou automatizados, os conhecidos **robôs/bots, não identificados como tal** para se passar por uma pessoa real e propagar desinformação nas rede sociais. Em períodos eleitorais, isso se torna mais comum ainda. Por isso, é importante checar a data de criação do perfil, a quantidade de seguidores, o uso de números e caracteres no nome de usuário para possível exposição e responsabilização.

Mas além das contas falsas, o que se verificou nas eleições de 2018 foi a agressão perpetrada também por grupos organizados, para ataques massivos.

Anonimato e bots também podem trabalhar para a democracia!

Anonimato

a identificação massiva de usuários não é uma saída democrática para combater práticas abusivas de desinformação. O anonimato é muito importante para perfis e ferramentas de denúncia, como o ***Sleeping Giants Brasil***, que expõe empresas que anunciam em sites que disseminam discurso de ódio e desinformação, solicitando que deixem de financiá-los com suas publicidades.

Bots

Lembramos ainda que não existem apenas robôs/bots do mal, que realizam ataques massivos, mas também existem bots cívicos, que favorecem a fiscalização e exercício de direitos, e até mesmo bots que servem para fiscalizar e denunciar outros bots! Como é o caso do ***Bot Sentinel***. Uma lista constantemente atualizada de bots amigos está disponível ***aqui***. O importante é que os usuários saibam quando estão interagindo com um - ou seja, o problema é quando grupos organizados usam bots para se passar por pessoas que não existem e ampliar a repercussão e alcance de conteúdos falsos.

Proteção de dados pessoais e privacidade

O aprimoramento das capacidades tecnológicas de coleta, processamento e armazenamento de dados, combinado com sua incorporação em ferramentas de marketing digital, favoreceu a crescente adoção por campanhas eleitorais de estratégias de marketing digital que se valem do uso de dados pessoais de eleitores.

Pesquisas recentes revelam como dados pessoais têm sido utilizados por campanhas para conhecer melhor seu potencial eleitorado, definir narrativas e mensagens, direcionar e microdirecionar[1] anúncios políticos, se comunicar com eleitorado, enviar propaganda eleitoral, material de campanha e até disseminar desinformação ("***Personal Data: Political Persuasion***" - Tactical Tech, 2019).

1 micro-direcionamento é o direcionar anúncios de acordo com perfilamento criado algoritmicamente com base em grande quantidade de dados pessoais

A possibilidade de uma comunicação mais direcionada, que atinja uma parcela do eleitorado que tenha maior afinidade com o projeto político de determinado candidato, já chegou a ser até uma promessa de maior eficiência na comunicação para campanhas menores e com recursos limitados. Contudo, há controvérsias, pois é necessário aplicar quantia substancial de recursos nessas plataformas para que publicações direcionadas, com impulsionamento pago, tenham alcance, e pouco se sabe do seu impacto eleitoral. Por outro lado, já se observou como a possibilidade de distribuir anúncios via Google AdSense tem gerado recursos para sites de redes de extrema direita.

Ninguém esquece o escândalo da empresa Cambridge Analytica, que utilizando dados de usuários do Facebook cedidos pela própria plataforma foi acusada de interferir nas eleições norte americanas - caso que até obrigou o CEO do Facebook a depor no Congresso estadunidense.

No Brasil, a pesquisa "***Dados e Eleições 2018***", realizada pela Coding Rights em parceria com a Tactical Tech, revelou um mercado brasileiro mal fiscalizado de data brokers e empresas de marketing digital, que oferecem serviços para campanhas baseados na construção de inteligência sobre eleitores, na segmentação desses eleitores em grupos e no micro direcionamento de conteúdos, por meio do uso de grandes bancos de dados pessoais formados a partir de bancos de dados públicos, da análise de mídias sociais, de pesquisas internas e de outros bancos de dados adquiridos de terceiros ou recebidos de clientes.

Os próprios "disparos em massa", que ocorreram nas eleições de 2018 em aplicativos de mensagens privadas, como o WhatsApp, nunca teriam sido possíveis sem o tratamento de números de telefone dos destinatários dos disparos ("***Santinhos, memes e correntes: um estudo sobre spam político no WhatsApp***" - InternetLab, 2019).

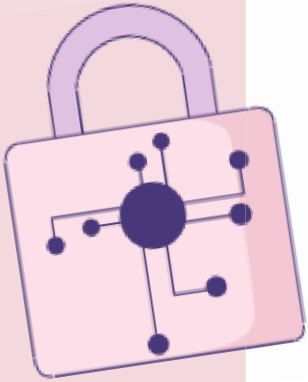
Vale ressaltar que a formação de bancos de dados com informações de eleitores e apoiadores e a busca por conhecer melhor o eleitorado em potencial não

são práticas novas em campanhas políticas. O que é novo é a incorporação de novas capacidades tecnológicas, que aumentam significativamente as possibilidades de coleta e análise de dados, não só em termos quantitativos mas, principalmente, qualitativos.

Este ano, com o início da vigência da Lei Geral de Proteção de Dados no Brasil em agosto, ainda a tempo das eleições de 2020, é fundamental que os princípios e regras trazidos pela nova lei sejam observados pela Justiça Eleitoral. E que todos os atores envolvidos no processo eleitoral, das campanhas às agências de marketing digital, entre outros, se adequem em relação ao uso e tratamento dos dados pessoais dos eleitores de todo o país.

Vale lembrar que, antes mesmo da vigência da LGPD, o Marco Civil da Internet já trazia, desde sua aprovação, em 2014, um conjunto de normas para o tratamento de dados no ambiente virtual, que foram aos poucos sendo incorporados nas resoluções do Tribunal Superior Eleitoral.

Uma campanha eleitoral preocupada com nossa privacidade deve:



- **Promover transparência** sobre práticas de uso de dados pessoais, garantindo ao eleitorado informações claras sobre dados coletados e finalidade de seu tratamento, assim como ofertando mecanismos de descadastramento para recebimento de informações e materiais da campanha;
- **Conhecer as bases legais** para tratamento de dados durante a campanha, incluindo a utilização de emails e de números de celular por candidaturas;
- **Não praticar e coibir,** dentro de seus partidos, práticas abusivas

em relação à privacidade dos eleitores – como o uso de disparos em massa sem consentimento em serviços de mensageria privada, doação, cessão e venda de bancos de dados pessoais a candidaturas;

- **Não utilizar dados sensíveis** como origem racial ou étnica, convicções religiosas, filiação a sindicatos ou organizações de caráter religioso e dados referentes à saúde ou à vida sexual para o direcionamento de propaganda eleitoral sem o expresso e informado consentimento dos eleitores destinatários das mensagens;
- **Promover maior transparência** sobre práticas de campanhas político-eleitorais que envolvam a contratação de empresas corretoras de dados, com informações sobre as empresas contratadas, as bases de dados utilizadas e o período de guarda desses dados.

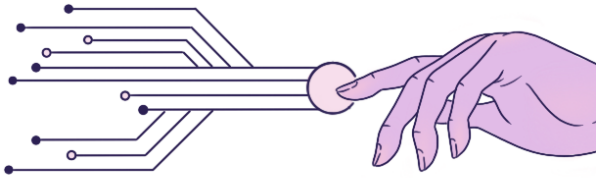
Por fim, é importante lembrar que o acesso a dados pessoais também tem sido utilizado para atacar candidaturas e vozes dissidentes. Por exemplo, a prática de *doxxing* (exposição de dados pessoais como endereço, número de telefone, dados de familiares etc.), fomentando ataques e até mesmo atos de violência física contra a pessoa exposta, tem sido cada vez mais utilizada como forma de violência política, não só contra candidaturas, mas também contra jornalistas.

Por essa razão, entre todas as mencionadas acima, qualquer candidatura tem a obrigação de cuidar também da segurança de seus dados e das bases de dados que constrói ao longo da campanha.

PODEMOS USAR AS TECNOLOGIAS PARA NOS PREVENIR DE ATAQUES?

Ninguém nunca está 100% seguro/a, nem na rede ou fora dela. Mas sempre podemos tomar alguns cuidados para estar mais protegido/as. A ideia de que "é melhor prevenir do que remediar" também serve para nossas interações digitais. Para isso, trazemos algumas dicas baseadas em experiências de oficinas realizadas pela Rede Transfeminista de Cuidados Digitais, focadas em modelo de ameaça de candidaturas.

Modelo de ameaças



A principal ferramenta utilizada por quem pensa táticas de segurança digital não é um software ou nenhuma tecnologia avançada. É o que chamamos de "modelo de ameaça"[2] ou "mosaico de ameaças"[3].

Já sabemos que ataques online também são moldados por discriminações de gênero, raça, sexualidade[4], classe, territorialidade, entre outras interseccionalidades. Sendo assim, os riscos e ameaças mudam de acordo com quem somos, onde estamos, o que comunicamos e por que meios.

2 Algumas sugestões de guias que ajudam a fazer o exercício de modelo de ameaças: "Surveillance Self-Defense, Modelo de ameaças", EFF: https://ssd.eff.org/pt-br/glossary/modelo-de-amea%C3%A7a ; "A guia de facilitação e aprendizagem em segurança da informação", Escola de Ativismo, 2017: https://escoladeativismo.org.br/wp-content/uploads/2018/08/AGUIA-DIGITAL-_-V7.pdf

3 "Guia Prática de Estratégias e Táticas para a Segurança Digital Feminista" - CFEMEA, 2017: https://feminismo.org.br/guia/guia-pratica-seguranca-cfemea.pdf

4 A pesquisa "Visibilidade Sapatão nas Redes: entre violência e solidariedade" ressalta as particularidade de ataques à mulheres lésbicas e suas interseccionalidades. https://medium.com/codingrights/visibilidade-sapat-c3-a3o-na-rede-52a2c54a1e45

Fazer um modelo de ameaças de uma candidatura é basicamente juntar a equipe para entender o contexto em que cada campanha opera. O quadro abaixo serve como um bom guia para esse tipo de conversa. É só juntar pelo menos a equipe de comunicação da campanha e listar.

- **Ameaças** são elementos externos que podem nos causar dano, por exemplo, milícias digitais espalhando a chamadas fake news, ou muitos dos ataques que listamos como formas comuns de violência política.
- **Vulnerabilidades** são aspectos internos à campanha que podem deixar a equipe mais sujeita a ataques. Por exemplo, senhas fracas, roubo de celular, pouco conhecimento em cuidados digitais.
- **Oportunidades** podem ser internas à campanha ou externas (do contexto e conjuntura). Por exemplo: se aproximar de outras candidaturas de mulheres, pessoas negras, LGBTQIA+, de outros grupos identitários e do partido para formar ou buscar redes de apoio.
- **Potências** são internas da campanha, como ter parte da equipe antenada em tecnologias.

É possível fazer um mosaico de ameaças em geral, inclusive físicas, ou para cada tipo de ação de comunicação em meios digitais. **Esse tipo de exercício também serve para iniciar conversas de cuidados digitais com a equipe da campanha**, conscientizar de que esse é um **tema importante e estratégico e traçar acordos.**

Quem somos? O que comunicamos? Para quem? Onde?

ex. candidatura / posição sobre direitos LGBT / público em geral / no facebook/insta/twitter

ex. candidatura / agenda da candidata / equipe da campanha / no grupo de chat

EXTERNAS			INTERNAS
	Ameaças	Vulnerabilidades	
	Oportunidades	Potências	

Quadro para mosaico de ameaças utilizado em oficinas pela Rede Transfeminista de Cuidados Digitais

Esse exercício é uma maneira de **prever situações e planejar respostas possíveis a essas ameaças, que sejam compatíveis com as oportunidades e potências do grupo.** Evita-se, assim, entrar em qualquer paranóia diante de todas as vulnerabilidades e tipos de ataques possíveis. A idéia é poder **focar em prioridades de segurança digital** que sirvam para mitigar os riscos mais prováveis que forem mapeados de acordo com o **contexto,** traçar um plano de ação caso aconteçam ataques e criar alguns acordos conjuntos, pois **segurança digital depende de ações de cuidado coletivo.**

Para além deste exercício, existem pelo menos **dois sites interativos** que também ajudam a fazer modelos de ameaça voltados para segurança digital. Infelizmente, nenhum deles em português, mas vale visitar:

- **Modo a prueba de riesgos** (em espanhol): https://modeladoriesgos.asuntosdelsur.org/
- **Security planner** (em inglês): https://securityplanner.org/

Cabe lembrar que, dado o contexto violento em que se faz política no Brasil, **algumas ameaças também abrangem segurança física e emocional**[5]**,** áreas importantes da ***segurança holística***[6], mas que não serão abordadas nesta cartilha. Encorajamos conversas específicas sobre esse tema tão sensível, com lideranças de seu partido e grupos de que você participe.

Dicas básicas de cuidados digitais preventivos

Seja qual for o resultado do modelo de ameaças, existem também dicas básicas que toda a equipe da campanha, sobretudo quem lida com informações sensíveis ou opera as plataformas de redes sociais, deve considerar como ponto de partida:

Senhas fortes por todos os lados

O primeiro passo da segurança digital passa sempre por **senhas fortes, diferentes para cada serviço e que mudam de tempos em tempos**[7]**.** Como fazer para garantir essas três características e administrar todas essas senhas? Vale ter um **chaveiro/gerenciador de senhas** para a equipe da campanha, o que facilita também alterar e compartilhar um novo bloco de senhas de tempos em tempos. Indicamos o KeepassXC (que funciona no computador em Windows, Linux, MacOs - ***dicas de como instalar KeePassXC***). Existem outros chaveiros, mas que, por funcionarem apenas online, estão sujeitos a mais vulnerabilidades.

5 Existem manuais de cuidados tratando também de questões de segurança física e emocional: "Physical, emotional and digital protection", Frontline Defenders, 2019 https://www.frontlinedefenders.org/en/resource-publication/physical-emotional-and-digital-protection-while-using-home-office-times-covid

6 Holistic Security, Tactical Tech: https://holistic-security.tacticaltech.org/introduction.html

7 Diferentes manuais com dicas simples de como criar senhas fortes: "Abre-te sésamo: as senhas da nossa vida digital", Boletim Antivigilância, 2017, disponível em: https://medium.com/codingrights/abre-te-s%C3%A9samo-as-senhas-da-nossa-vida-digital-469a8772723a; "Guia Autodefesa", disponível em: https://guia.autodefesa.org/senhas.html "Guia Prática de Estratégias e Táticas para a Segurança Digital Feminista" - CFEMEA, 2017, disponível em: https://feminismo.org.br/guia/guia-pratica-seguranca-cfemea.pdf#Cfemea-CorrecaoFinal_A.indd%3A.34963%3A1275

É muito fácil decifrar senhas que são baseadas em informações públicas, como data de aniversário ou animal de estimação. Senhas longas com palavras inventadas ou desconexas, por exemplo, são muito mais seguras. Além disso, vazamentos de dados de grandes serviços de Internet (incluindo senhas e contatos de e-mails, inclusive) tem sido bem frequentes. Se você usar a mesma senha para tudo, o vazamento de um serviço pode comprometer várias de suas contas. Neste link ***https://haveibeenpwned.com/*** dá até para saber se a senha de alguns de seus emails já vazou por aí. Enfim, de vazamentos a zolhudos, temos razões de sobra para mudar nossas senhas periodicamente. Para além de contas em serviços online, lembrem-se de habilitar senha nos seus dispositivos. **Celular sem senhas, jamais!**

Autenticação de dois fatores para evitar roubo de contas

Roubo de contas tem sido um ataque bem comum. Para se proteger, ter dois tipos de senhas para acessar uma conta pode ajudar bastante. É por isso que muitos serviços, dos apps de chat às redes sociais, disponibilizam autenticação de dois fatores. Quando habilitada, um código é enviado por SMS ou email, servindo como um passo a mais de segurança para o processo de login. Assim, se a senha vazar, intrusos não invadem tão facilmente.

Habilitem autenticação de dois fatores principalmente nas redes sociais da campanha. Garantam que o número de telefone que recebe essas mensagens de autenticação seja de alguma pessoa que tenha práticas de cuidados digitais e, quando habilitar esse recurso, não se esqueça também de buscar como emitir um código de backup e guardar em lugar secreto e seguro. Assim, se o celular for perdido, também é possível acessar a conta com esse código.

Criptografia para proteger comunicações e armazenar dados

A criptografia é uma forma de codificar conteúdos e assegurar que só quem tenha a chave criptográfica possa acessá-los. Ela serve para reforçar a segurança de nossas comunicações e do armazenamento de informações[8]. Então, para evitar "boi na linha", opte por canais de comunicação que usam criptografia. Se formos falar apenas em apps de mensagem, é bom lembrar que grupos de mensagem do Telegram, por exemplo, não têm criptografia.

Se você faz backup das suas mensagens de WhatsApp guardando na nuvem, também não tem. Além disso, habilitar o backup do zap faz com que seus dados passem a ser compartilhados do Facebook, dono do Whatsapp, para o Google, dono do Drive. Nesse sentido, o Signal é o aplicativo de mensagens que é a opção mais recomendada, mas não só pela questão da criptografia[9].

8 Para saber mais sobre a importância da criptografia nas nossas vidas: "A importância social e econômica da Criptografia" - Coalizão Direitos na Rede, 2020

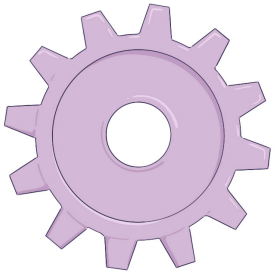
9 Para entender melhor qual a diferença na segurança de cada app de chat: Whatsapp x Telegram x Signal: como escolher?, Escola de Ativismo, 2019: https://medium.com/cuidados-integrais/whatsapp-x-telegram-x-signal-como-escolher-a0793c3e190c; SaferManas, Apps de Chat, 2018: https://www.codingrights.org/wp-content/uploads/2018/05/01_safermanas_pt.gif; Do sexxting ao grupo de família: chats criptografados para todxs, Boletim Antivigilância, 2017: https://medium.com/codingrights/do-sexxting-ao-grupo-de-fam%C3%ADlia-chats-criptografados-para-todxs-46109f22183f

O quadro abaixo compara os apps de mensagem mais usados e deixa claro porque **o Signal é o preferido, inclusive para evitar grampos:**

É código aberto e verificado	⊖	⊖	⊖	!	✓
Criptografia fim-a-fim	⊖	✓	!	!	✓
Mensagens auto-destrutivas	⊖	⊖	⊖	!	✓
Chamadas seguras (encriptadas fim-a-fim)	⊖	✓	⊖	⊖	✓
Sigilo do número Telefônico	✓	⊖	⊖	✓	✓
Autenticação de dois fatores	!	✓	⊖	✓	✓
Senha para abrir app	!	⊖	⊖	✓	✓

Legenda: ✓ Sim ⊖ Não ! Depende

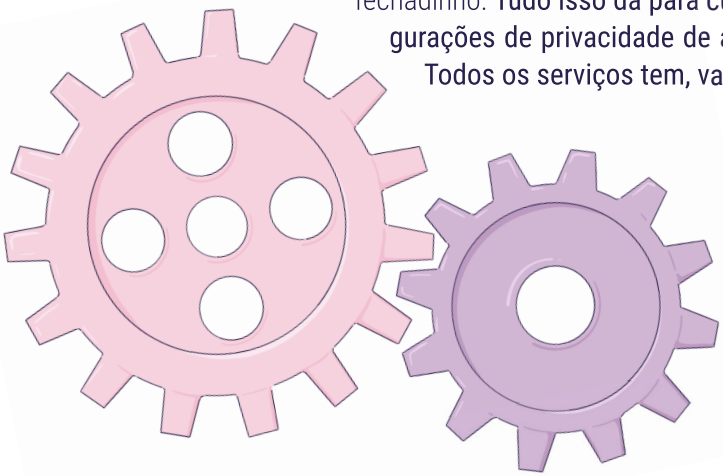
Para além dos canais de comunicação, proteja também sua conexão usando **VPNs (Rede Virtual Privada), que mantém nossos dados seguros por criptografia enquanto trafegam na rede. Uma VPN é aconselhável principalmente para quem usar WI-FIs compartilhados, como num café.** A comunidade do Rise Up disponibiliza uma VPN gratuíta: ***https://riseup.net/en/vpn***. **E proteja o armazenamento dos seus arquivos *habilitando criptografia de disco*, inclusive nos seus dispositivos**. Assim, se perder o celular, vai ter menos dor de cabeça.



Configurações de privacidade e segurança: estamos compartilhando mais informações do que é preciso? Qual nosso rastro digital?

Como as empresas de Internet ganham com nossos dados, o mais comum é que as configurações de privacidade de aplicativos e redes sociais estejam habilitadas, por padrão, para o compartilhamento excessivo de informações, seja com outras pessoas ou com essas plataformas.

Mas vale sempre se perguntar: estamos compartilhando mais informações e com mais gente do que é preciso? Por exemplo, precisamos mostrar a localização de nossos posts? Preciso guardar histórico de localização, áudios etc.? Que apps realmente precisam ter acesso ao meu microfone? Quem está vendo meus posts? Um/a candidato/a pode querer ter, por exemplo, um perfil pessoal e um outro da candidatura, sendo que o pessoal pode ser mais fechadinho. **Tudo isso dá para customizar nas configurações de privacidade de apps e plataformas. Todos os serviços tem, vale checar um a um.**



Cheque suas configurações de privacidade!

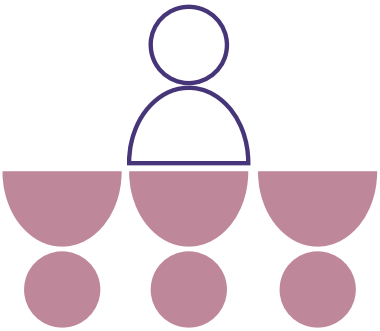
- **Google:** https://safety.google/intl/pt-BR/privacy/privacy-controls/
- **Facebook:** https://www.facebook.com/help/443357099140264
- **WhatsApp:** https://faq.whatsapp.com/general/security-and-privacy/how-to-change-group-privacy-settings/?lang=pt_br
- **Telegram:** https://telegram.org/faq/br
- **Instagram:** https://help.instagram.com/196883487377501
- **Twitter:** https://help.twitter.com/pt/safety-and-security#ads-and--data-privacy
- **Tik Tok:** https://support.tiktok.com/pt/privacy-safety/comment--duet-and-direct-message-control-default
- **Apple:** https://www.apple.com/privacy/manage-your-privacy/
- **Microsoft**: https://account.microsoft.com/account/privacy?refd=privacy.microsoft.com&destrt=privacy-dashboard&lang=pt-PT

Entre outros...

Revisar as configurações de segurança de serviços online também é importante. No ***check up de segurança do Google***, por exemplo, você também pode checar que dispositivos estão conectados nas sua conta e nas contas da campanha. É sempre bom fazer uma limpeza de vez em quando. **Por exemplo, dispositivos antigos, perdidos ou de pessoas que já não fazem parte da equipe da campanha podem ser removidos do acesso.**

Por fim, é comum termos contas esquecidas por aí, mas, justamente por estarem esquecidas, elas acabam virando pontos de vulnerabilidades. O serviço ***https://deseat.me*** ajudar a **desabilitarmos contas registradas no nosso email que não usamos mais. Limpeza serve tanto para a saúde física, como para a digital.** Quanto menos dados nossos estiverem por aí, menos expostos/as ficamos para práticas como *doxxing* (exposição de dados pessoais), *stalking* (perseguição persistente) etc.

Gestão de identidades: em uma, já somos muitos/as



Nas suas origens, a Internet fomentava o exercício de múltiplas identidades. Como bem diz a guia "***Seja monstra: identidades para nossa vida cotidiana***", era um "espaço onde podíamos criar diferentes experiências de si". Mas a lógica das redes sociais quebrou isso, nos empurrou para uma narrativa bastante lucrativa para os modelos de negócio extrativistas de dados pessoais, no qual operam essas plataformas: a ideia de que nossa confiabilidade está ligada a ter um único perfil atrelado ao nosso nome do RG, com informações pessoais atualizadas o tempo todo. Mas não precisa ser assim, como mostra a guia, que transpõe o conceito de "corpo monstro", cunhado pela pensadora Jota Mombaça, para a discussão sobre o direito de pessoas LGBTQIA+ optarem por momentos de privacidade e outros de visibilidade:

> "**Jota Mombaça descreve o corpo em si como um monstro,** um produto dos discursos e construções sociais que está sempre se transformando e desafiando as definições que tentam classificá-lo. Ser monstro é abraçar a multiplicidade de identidades que existem em nós e ir além disso, sabendo que identificação e transgressão nunca acontecem separadas."
>
> *(Seja monstra: identidades para nossa vida cotidiana)*

Essa lógica também se aplica a equipe de campanhas eleitorais. **Em um contexto violento e polarizado, às vezes pode ser saudável, e até estratégico, separar um pouco as nossas identidades privadas das públicas e profissionais nos perfis dessas redes sociais. Ou mesmo, as identidades coletivas das pessoais**[10].

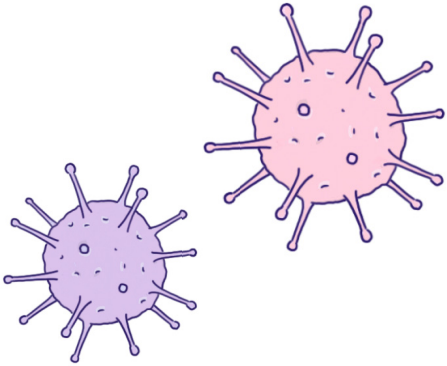
Os perfis da campanha são identidades coletivas. Vale pensar o quanto se quer atrelar essa identidade às identidades pessoais da equipe da campanha, por exemplo, à administração desses perfis. Já vimos que, principalmente no Facebook, tem sido um tipo de ataque bastante comum visar administradores de páginas pelo fato de seus perfis pessoais serem os mesmos que gerem essas páginas. Nesse sentido, vale também pensar em **restringir a quantidade de pessoas que precisam ter direitos da administração das contas de redes sociais; quanto menos, mais seguro para todo o grupo.**

Em alguns casos, vale até pensar: que tal um perfil privado, só com pessoas mais próximas, que você realmente conhece? E outro mais aberto, para atuação política? O mesmo vale para números de WhatsApp, endereços de e-mails etc. (***dicas de como ter duas contas de WhatsApp em um celular***).

Esse tipo de gestão pode dar um trabalhinho extra, mas vai diminuir o impacto de ataques online. Assim, se seu perfil político é alvo de ataques e bloqueios, você ainda tem uma persona online com suas pessoas próximas, que importam. Trata-se de algo bem diferente de criar perfis falsos para enganar as pessoas, pois todos esses perfis são parte da sua persona.

10 Mais informações sobre táticas de gestão de identidade: "Creando y gestionando identidades" - Gendersec.tacticaltech.org wiki, 2015: https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual/es#Creando_y_gestionando_identidades_en_l.C3.ADnea

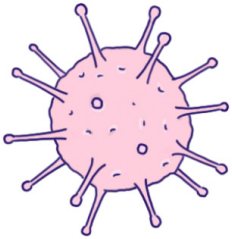
Cuidado no click! Malware e vírus

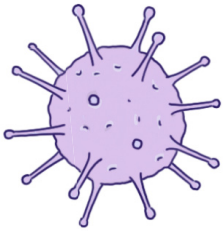


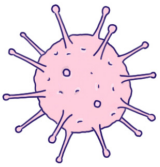
Uma tática comum para roubar senhas ou instalar *malwares* são os ataques de "phishing" (do inglês "pesca"). Normalmente, são mensagens que tentam nos convencer a clicar num link, abrir um documento, registrar nosso nome de usuário e senha em algum site falso ou até a instalar algum programa.

É comum que essas mensagens tentem se passar pelo seu banco, ou suporte técnico de algum serviço online. Se a gente cair no truque, podemos enviar nossa senha para um agente malicioso ou, se algum *malware* for instalado, nossos dispositivos podem ser controlados de forma remota.

Para evitar cair nesse ataque, **é importante manter o software de seus dispositivos sempre atualizados**, pois o fabricante sempre traz atualizações de segurança que combatem os malwares mais comuns. **Observe sempre os remetentes de emails que te enviam links** e, se tiver dúvidas, contate a pessoa antes de clicar em algo. **Não baixe arquivos ou clique em links em emails provenientes de desconhecidos** (*mais dicas de como lidar com phishing*).







Sistemas atualizados e backups seguros

Atualizar seu sistema operacional e manter backups (cópia de segurança) de seus dispositivos são medidas preventivas que devem fazer parte da rotina sem requerer muito trabalho, principalmente porque podem ser automatizados. Se tiver possibilidade, também vale pensar em **backups do site da campanha, de conteúdos que a candidatura posta em redes sociais** (caso o perfil seja bloqueado, já pensou que triste perder todas as lives?) e de outros arquivos online.

Prepare-se em caso de perda de celular

Nada mais comum no Brasil do que ter o celular roubado ou perdido. Mas dá para se preparar para esse tipo de dor de cabeça. Além de fazer backups seguros, existem **apps que localizam, travam e apagam toda a informação do celular perdido**: ***Find my Device*** (android) e ***Find my iPhone*** (iphone). **Habilite e teste antes de precisar**. Em caso de perda, lembre-se de remover o acesso desse dispositivo nas configurações de segurança que mencionamos anteriormente.

Zoombombing: ataque em videoconferências

O contexto de quarentena e isolamento social gerou uma profusão de eventos online em plataformas de videoconferência. Apesar de algumas vulnerabilidades de segurança - como ***compartilhar dados do seu dispositivo iOS com o Facebook***, mesmo que você não tenha conta lá, e ***falhar na segurança de senhas*** de reuniões privadas - além de ***não ter criptografia ponta-a-ponta***, o Zoom tem sido a plataforma mais escolhida e também a mais atacada. Daí o nome "zoombombing" para se referir às invasões de salas para propagar áudios e vídeos violentos. Mal começou e já tivemos incidentes de zoombombings em algumas reuniões de pré-campanha por aqui no Brasil, principalmente de mulheres negras.

Para se prevenir, o primeiro passo é se perguntar: precisa usar o Zoom mesmo?

Se o evento é uma **transmissão online aberta ao público e não precisa que todas as pessoas que assistem participem com áudio e vídeo, certamente, o Zoom não é a melhor opção.** Para transmissão de lives e eventos, opte por ferramentas de streaming como StreamYard *(dicas de como usar StreamYard para fazer lives)*, que transmite simultaneamente o seu bate papo nos canais de redes sociais da campanha. Se tiver transmitindo para o Youtube, vale habilitar *ferramentas de moderação de chat* antes de começar sua live, assim vocês ficam preparados para bloquear qualquer ataque em massa de comentários agressivos.

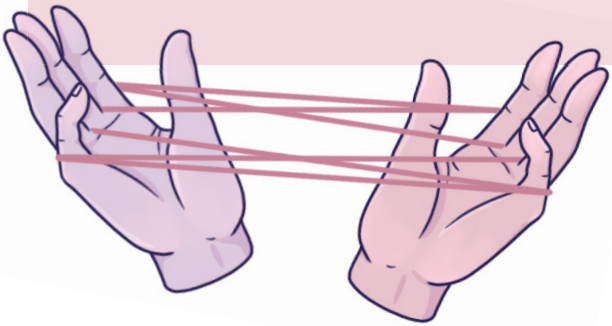
Se o objetivo é uma **reunião fechada**, outros serviços, como o *JitsiMeet* e *Big Blue Button* são mais seguros e usam criptografia, mas funcionam melhor se instalados em servidor próprio, o que pode ser um problema para quem não tem pessoa técnica na equipe. Existem alguns coletivos focados em cuidados digitais que hospedam variações do JitsiMeet também. E o serviço funciona bem, mesmo sem servidor próprio, para reuniões com poucas pessoas. Outra alternativa é o GoToMeeting, que oferece serviço criptografado por três meses gratuitos. Em todos os casos, cuide bem do link da reunião, ele continua sendo a chave da sua sala.

Alguns exemplos de servidores comunitários de para hospedar suas sala do JitsiMeet:

- meet.jit.si
- meet.mayfirst.org
- meet.greenhost.net
- vc.autistici.org
- framatalk.org
- calls.disroot.org
- meet.guifi.net
- meet.collective.tools

Mas se a campanha precisa mesmo do Zoom (porque precisa de muita, muita gente na sala ou porque a lógica é poder abrir discussões em grupos menores no meio da reunião maior, ou qualquer característica que você considera que só tem no Zoom), tome alguns cuidados ao configurar a sala. **O link é a chave da sua sala, não divulgue em redes sociais; peça que as pessoas se cadastrem e envie o link e senha por essa lista de pessoas cadastradas**. Nas configurações de reunião (Minha conta > Configurações > Reunião), considere **desabilitar bate-papo privado, transferência de arquivos, compartilhamento de tela para além da anfitriã e desabilite a permissão de que participantes removidos reingressem na sala. E habilite sala de espera** (para moderar quem entra, antes de entrar). Antes de iniciar a reunião, **a pessoa que for anfitriã precisa estar preparada para ataques, pelo menos sabendo acalmar participantes e localizar onde desativar o microfone de todos, desativar a câmara dos invasores, expulsar pessoas da sala e bloquear novas entradas.** Também é aconselhável designar uma segunda pessoa para documentar eventuais ataques por meio de gravação e/ou capturas de tela. Mais dicas para configurar o zoom: *https://escoladeativismo.org.br/como-se-defender-de-um-ataque-no-zoom/*

Cuidados digitais são pensados em coletivo. Se a equipe da campanha seguir junta esses passos, estarão todos/as um pouquinho mais seguros/as e precavidos/as em caso de ataques.



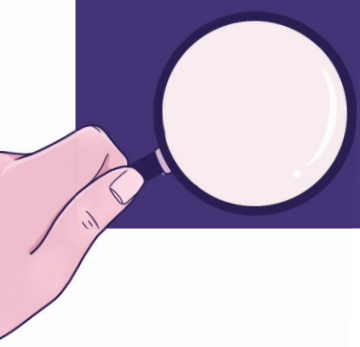
Essas são algumas dicas básicas, considerando algumas atividades comuns às campanhas. Mas não é uma lista exaustiva. Para seguir avaliando e evoluindo nessas práticas de cuidados, indicamos consultar o site *"#SeguridadDigital: Que Mercúrio retrógrado no afecte tus comunicaciones digitales!"* (em espanhol). De maneira divertida, o site faz algumas perguntas para avaliar suas práticas de cuidados e depois te dá algumas cartas sugerindo melhorias. Dá até para se inscrever para receber metas da semana, com dicas de como implementar melhorias, respeitando o seu ritmo.

Guias bastante acessíveis com dicas de segurança

- *Cfemea: Guia Prática de estratégias e táticas para a segurança digital feminista*
- *Guia de Autodefesa Digital*
- *EFF: Autodefesa contra a vigilância: dicas, ferramentas e tutoriais para uma maior segurança nas comunicações online*
- *#SaferManas: dicas de cuidados digitais em formato de gifs*
- *Security Planner: Planejamento de Segurança (em inglês)*
- *Modo a prueba de riesgos (em espanhol)*
- *Ciberseguras*
- *Frontline defenders (em ingles)*
- *Seja monstra: identidades para nossa vida cotidiana*

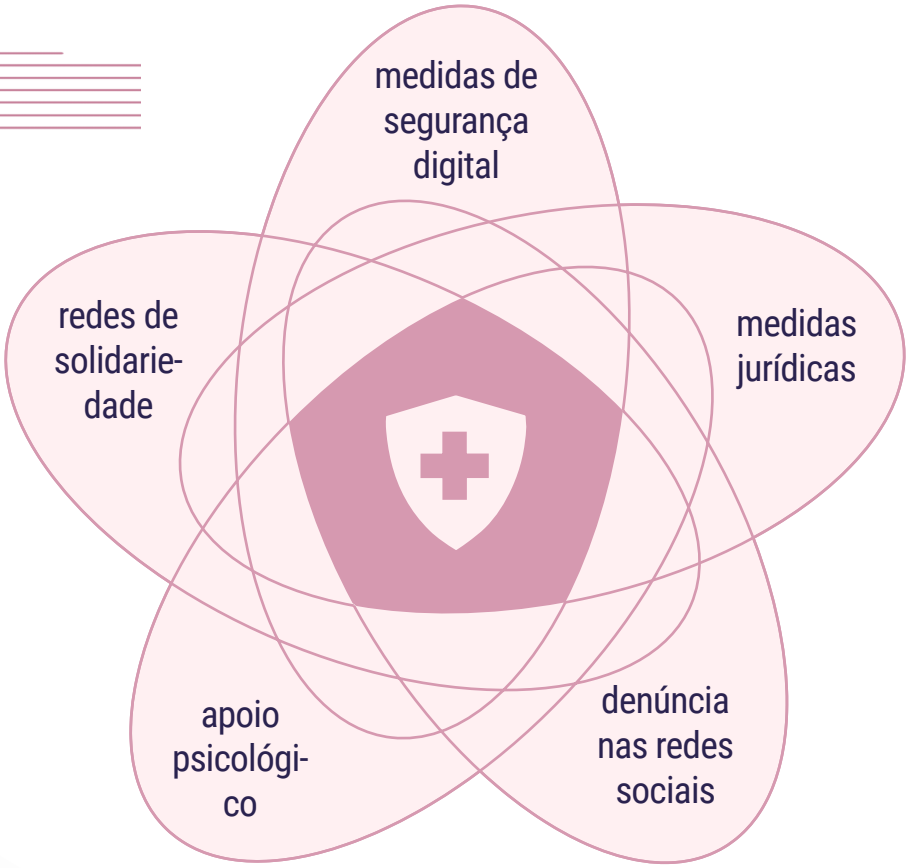
Guias para consultar em casos de ataques

- *Kit de primeiros socorros digitais*
- *AccessNow Helpline*
- *Acoso.Online: Pornografia sem consentimento: Cinco recomendações para denunciar e resistir com a sua publicação*

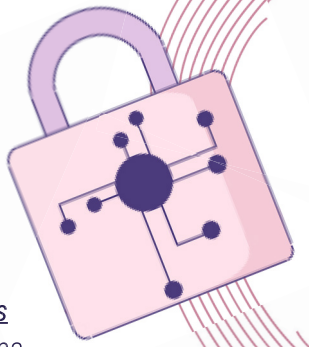


O QUE FAZER EM CASO DE ATAQUES?

Ataques online sempre requerem soluções em várias áreas: medidas de segurança digital, medidas jurídicas, medidas em interlocução com as redes sociais, além de apoio psicológico e de nossas redes de solidariedade. Um bom plano de mitigação de ataques considera todos essas camadas.



Medidas de segurança digital para mitigação de danos



Em caso de ataques ou situações estranhas acontecendo, **vale rever os passos das dicas básicas acima**. Para situações específicas, o site do "***Kit de Primeiros Socorros Digitais***" é uma ótima referência. O site te conduz por alguma perguntas com o objetivo de diagnosticar melhor o problema e sugerir algumas soluções técnicas para lidar com casos em que:

- Perdeu seu dispositivo
- Não consegue acessar suas contas
- Seu dispositivo está com comportamento estranho
- Recebeu uma mensagem suspeita
- Seu site caiu e não se sabe o que aconteceu
- Outra pessoa está se passando por você online
- Está sendo alvo de perseguição online
- Perdeu seus dados

Para problemas técnicos que não puderem ser resolvidos consultando esse guia, o kit também conta com uma lista de organizações de apoio para contato. Entre elas, a linha de ajuda da ***ONG Access Now***, que também oferece ajuda em português.

Atentamos para o fato de que essas linhas de auxílios são canais de organizações internacionais, que têm mais estrutura para dar apoio 24 horas por dia, 7 dias por semana. Mas sabemos que contexto também importa. Então, para além dos auxílios técnicos, indicamos que, em caso de ataques complexos, busquem também organizações e coletivos que tratam de segurança e cuidados digitais, bem como advogadas e advogados do seu entorno. Até porque, em muitos casos, o apoio técnico precisa caminhar junto do apoio jurídico.

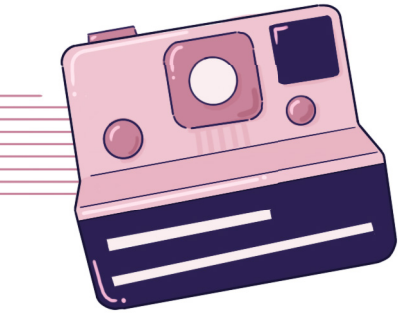
Denúncias nas plataformas

Para além de soluções técnicas, é comum que casos de ataques online também requeiram medidas tomadas pelas empresas detentoras das redes sociais. Todas elas têm mecanismos de denúncia para realizar pedidos de bloqueio ou remoção de conteúdos e perfis que tiveram comportamento ilícito ou em desacordo com os **Termos de Uso** desses serviços.

Existem ainda casos em que nossos conteúdos ou contas são bloqueadas pelos algoritmo das próprias plataformas. Seja por esse tipo de censura, pela falta de resposta a denúncias recebidas ou até por premiar com mais visibilidade conteúdos agressivos e remunerar disseminadores de ódio e desinformação, as plataformas acabam tendo também um papel na violência política. Portanto, cabe também sempre documentar todo o conteúdo que está sendo denunciado, pois nunca se sabe se o único caminho possível será o judicial.

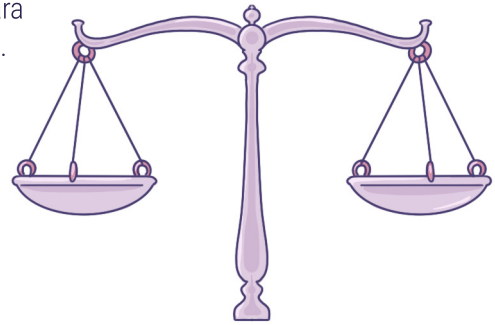
Documentação sobre o ataque

Umas das primeiras coisas a se fazer em caso de ataques é **guardar evidências** antes que os agressores deletem o conteúdo ou excluam a conta. Contudo, é indicado, até mesmo para preservar a saúde mental e psicológica da equipe, que, se possível, quem é o alvo principal do ataque não fique em contato direto com as manifestações desse ataque, nem seja o responsável por fazer a documentação. Isso pode causar stress e raiva, entre outras emoções tóxicas que desestabilizam a pessoa (justamente um dos objetivos de quem ataca), o que até pode prejudicar a documentação.



Então, dentro da equipe da campanha, indiquem uma pessoa que seja mais metódica, paciente e com estômago para documentar. Em caso de ataques de discurso de ódio, ameaças, desinformação, vazamento de dados, normalmente a

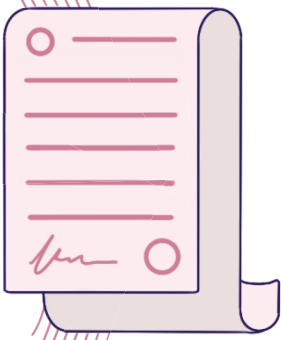
documentação inclui: tirar captura de tela (*printscreen*) da violência, do nome vinculado à página, listar links das postagens e dos perfis, baixar o conteúdo e, se possível e dependendo da gravidade, fazer registro em cartório, por meio de ata notarial. Ataques mais sofisticados podem precisar de apoio de especialistas de segurança digital para serem documentados. Tudo isso servirá como prova para os próximos passos, de procurar canais de denúncia e o Judiciário para uma resposta efetiva à violência política.



Denúncias no Judiciário

É muito comum que violências políticas que se manifestam nos meios digitais passem impunes ou nunca cheguem a ser judicializadas. Primeiro, porque há uma banalização das manifestações de violência online pela crença de que elas se atêm aos meios digitais. Mas não é verdade. **Existe um contínuo entre o online e o offline**, e hoje, mais do que nunca, ambos afetam várias esferas da nossa vida.

Além disso, a impunidade que perpassa a violência de gênero em geral, com todas as questões de machismo, re-vitimização e despreparo do sistema de Justiça, também atravessa a violência política de gênero na Internet. Acreditamos que também pode ser um papel político de candidaturas fazer com que esses casos não passem subnotificados e cheguem até o Judiciário. Portanto, listamos a seguir algumas previsões legais que podem auxiliar nesse movimento.



O que diz a legislação?

Casos de violência política na Internet podem ser enfrentados com recurso à Lei Geral de Proteção de Dados, ao Marco Civil da Internet, além de leis na esfera penal, com fundamento nos crimes cometidos contra a honra, lei antirracismo,

como nas esferas cível e eleitoral, com ações para remoção de conteúdo, aplicação de multas e pagamento de indenização.

Procedimentos para pedidos de remoção de conteúdo direcionados diretamente às plataformas, juntamente com a provocação de canais de denúncias do Judiciário ou da sociedade civil, também são alternativas. Reforçamos a necessidade de uma abordagem *"multissetorial"* da violência política, utilizando vários desses marcos legais para provocar respostas a um problema complexo. Ou seja, precisamos de várias ferramentas para enfrentar redes organizadas (milícias digitais) que praticam diferentes atos de violência política nas redes.

Antes de mais nada, é preciso ter em mente que é basilar um balanço entre liberdade de expressão e moderação de conteúdo - o objetivo aqui é combater conteúdos violentos, que silenciam candidaturas, sobretudo de mulheres e de grupos minorizados. Em muitos casos, é possível que o conteúdo divulgado esteja em desacordo com **os termos de uso e políticas de privacidade das plataformas**. Nestas situações, recomendamos primeiramente notificar a empresa para a remoção do conteúdo, denunciando na própria plataforma.

Além disso, também é dever das candidaturas seguirem as diretrizes da Lei Geral de Proteção de Dados Pessoais ao gerir as bases de dados de seu eleitorado, principalmente nas iniciativas de marketing político digital, bem como entender como essas previsões se harmonizam com o que determina também a Lei das Eleições sobre a construção de cadastros. Vejamos agora os mecanismos legais que estabelecem direitos e deveres para as campanhas eleitorais na Internet:

Marco Civil da Internet

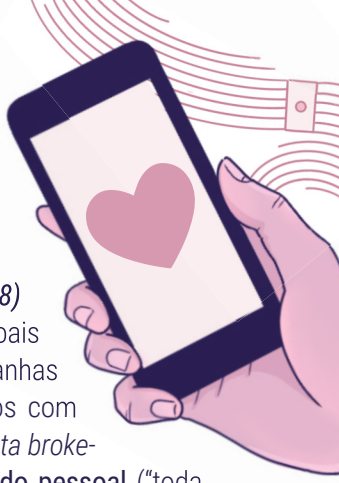
Uma das fontes legais de proteção é o Marco Civil da Internet (*Lei nº 12.965/2014*), que, para além de regras e princípios de direitos humanos para o uso da rede, dispõe sobre responsabilidade de intermediários sobre conteúdos publicados por terceiros. A regra geral é que plataformas estão isentas de responsabilização até que haja ordem judicial para remoção daquele conteúdo. Mas existem exceções: direitos auto-

rais e disseminação não consensual de imagens íntimas. Contudo, plataformas também removem conteúdos com base nos seus termos de uso, e o Marco Civil da Internet, infelizmente, deixou uma lacuna, não estabelecendo mecanismos que cobrem transparência dessas plataformas sobre quantos, quais e como conteúdos são removidos. Na prática, o que se tem observado é que muitos conteúdos de discurso de ódio permanecem online, enquanto conteúdos feministas ou identitários são bloqueados. Por exemplo, muitas ativistas lésbicas relatam terem seus posts censurados ao escreverem a palavra "sapatão", há muito tempo reapropriada pelo movimento ("***Visibilidade Sapatão nas Redes***" - Coding Rights, 2020).

O Marco Civil da Internet também trata de guarda obrigatória de registros de conexão e aplicação, instrumentos que podem ser utilizados em processos de investigação. O quadro a seguir ilustra as obrigações de guarda de acordo com tipo de registro, bem como os requisitos para acesso:

Tipo de dado de comunicação	Legislação	Tempo de guarda	Requisitos para acesso a esses dados
Logs de conexão (IP, data e hora de início e término)	Marco Civil e Regulamento (Decreto Nº 8.771)	1 ano. Mais tempo por cautelar de autoridade policial ou administrativa ou MP	Odem Judicial para informar processo civil ou penal. 60 dias para requerimento no caso de cautelar
Logs de aplicações (data e hora de início e término)	Marco Civil e Regulamento (Decreto Nº 8.771)	5 meses para provedor profissional (consentimento e finalidade) Outros podem ter que guardar por ordem judicial. Mais tempo por cautelar de autoridade policial ou administrativa ou MP. Não podem ser guardados pelo provedor de conexão.	Ordem judicial para informar processo civil ou penal
Fluxo de Comunicações telefônicas e de informática e Comunicações armazenadas	Protegido pelo Marco Civil. Acessível pela Lei da Interceptação	Prazo de 15 dias, renovável por 15 se comprovada indispensabilidade da prova	Ordem Judicial para informar investigação ou processo penal, sob segredo de justiça. Indício de Autoria, meio necessário, pena de reclusão. Polícia ou MP podem requerer.
Dados Cadastrais (qualificação pessoal, filiação e endereço)	Marco Civil e Reguamento (Decreto Nº 8.771). Projeto de Lei de Proteção de Dados?		Por requisição de autoridades administrativas com competência legal, dever de publicar relatório de requisições

Lei Geral de Proteção de Dados Pessoais (LGPD)



A Lei Geral de Proteção de Dados Pessoais (Lei 13718/2018) traz todo um regramento para tratamento de dados pessoais que pode incidir não só sobre o uso de dados por campanhas políticas, mas sobre toda uma gama de atores envolvidos com marketing político digital, como agências de marketing e *data brokers.* A lei adota em seu art. 5º uma definição do que é **dado pessoal** ("toda informação relacionada a pessoa natural identificada ou identificável") e do que é dado **pessoal sensível** ("dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural").

Destacamos aqui alguns artigos:

*** Art. 7º e Art. 11: estabelecem as hipóteses que autorizam o tratamento de dados pessoais e de dados pessoais sensíveis, respectivamente.** No caso do art. 7º, destacam-se, para o cenário eleitoral, a hipótese de tratamento mediante consentimento do titular e a hipótese de tratamento quando necessário para atender o legítimo interesse do controlador. Nesta última hipótese, a análise deve ser feita caso a caso considerando a legitimidade do interesse, a necessidade e adequação do tratamento, a legítima expectativa do titular quanto ao tratamento de seus dados, e as salvaguardas adotadas para garantir transparência e segurança. Já no caso do Art. 11, o dispositivo estabelece, no inciso I, que dados pessoais sensíveis só podem ser tratados mediante consentimento específico e destacado. Na hipótese de não haver consentimento, a lei fornece outras 7 bases legais, dentre as quais não se inclui o legítimo interesse do controlador.

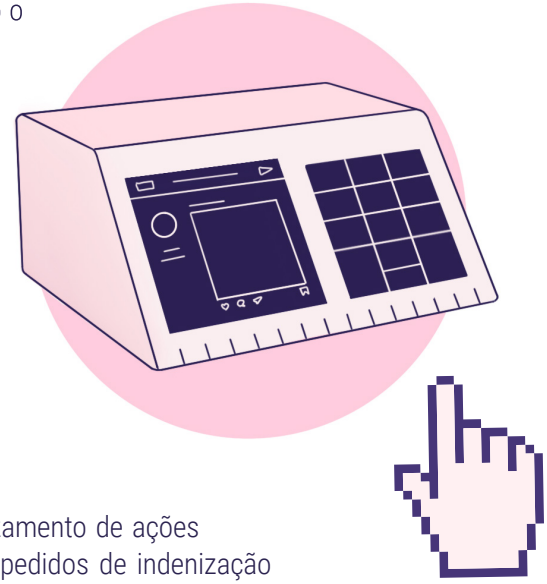
*** Art. 7º § 5º e Art. 9º: trazem previsões sobre compartilhamento de dados.** O art. 7º § 5º determina que o controlador deve obter consentimento do titular para comunicação ou compartilhamento de dados quando estes foram tratados com base no consentimento fornecido pelo titaular. Enquanto o art. 9º define que o titular tem direito ao acesso a informações acerca do uso compartilhado de dados pelo controlador.

Ainda, os princípios da LGPD definidos no art. 6º ganham uma relevância especial para a proteção de dados pessoais nas eleições deste ano. O princípio da finalidade, por exemplo, garante a realização do tratamento de dados para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior que seja incompatível com essas finalidades. No âmbito eleitoral, respeitar a finalidade do tratamento implica que bancos de dados constituídos para finalidades comerciais, para prestação de serviços de saúde ou para prestação de políticas públicas, por exemplo, não possam ser utilizados com finalidades político-eleitorais.

Já o princípio da necessidade garante que o tratamento de dados se restrinja ao mínimo necessário para a realização de suas finalidades, sem abranger dados excessivos em relação às finalidades do tratamento de dados, oferecendo uma baliza para avaliação de estratégias de campanha que se baseiam em uma coleta e análise excessiva de dados pessoais que excedam o necessário para estabelecer uma comunicação com o eleitorado. O princípio da transparência fomenta que campanhas informem seus eleitores e apoiadores a respeito dos dados coletados e para quais finalidades. Fundamental para a devida fiscalização cidadã e judiciária do processo eleitoral, a transparência deve abarcar inclusive a prestação de serviços para campanhas, pautando-se em iluminar quais os procedimentos que as campanhas estão tomando a partir de bancos de dados pessoais.

A aplicação principiológica da LGPD estabelece um diálogo inclusive com os art. 57-B, III e 57-G da Lei das Eleições, que determinam que candidatos, partidos e coligações devem construir cadastros de forma gratuita e oferecer mecanismo de descadastramento, no caso de envio de mensagens eletrônicas, servindo como norte interpretativo e reforçando a tutela dessas previsões. Em paralelo, a redação do art. 31 da Resolução 23.610/19, que regulamenta o art. 57-E da Lei das Eleições avança essa proteção ao vedar que pessoas jurídicas de direito privado cedam, usem ou vendam dados pessoais de seus clientes em favor de candidatos, partidos e coligações.

Avançar na maior responsabilização dos candidatos e partidos sobre os conteúdos que circulam é um desafio em 2020. Para coibir possíveis abusos que ameacem a igualdade de chances e direitos fundamentais, realizar denúncias às plataformas e agentes do sistema de Justiça Eleitoral, como o Ministério Público, é fundamental - todos esses atores devem estar atentos ao cumprimento dos dispositivos legais articulados nessa cartilha.



Legislação Eleitoral e Propaganda Irregular

No âmbito cível, é possível o ajuizamento de ações para remoção do conteúdo, e de pedidos de indenização por danos morais e materiais causados, com base na violação de direitos da personalidade, como a honra e a imagem da vítima, sem prejuízo de outras providências na seara penal e eleitoral.

Direito de Resposta *Lei nº 13.188/2015*

Garantia dada a partidos políticos, coligações ou candidaturas, a contar das convenções partidárias, de se defenderem de ofensas ou fatos sabidamente falsos veiculados em propaganda eleitoral ou pela imprensa em geral, reparando sua honra ou retificando informações.

Assim, sob o aspecto do direito eleitoral, a depender da gravidade da conduta, é possível ajuizar ações de Impugnação do Registro da Candidatura (AIRC), Ação de Investigação Judicial Eleitoral (AIJE), Ação de Impugnação de Mandato Eletivo (AIME) perante a Justiça Eleitoral, quando for constatada influência do poder econômico, desvio e abuso de poder (inclusive o religioso) ou uso indevido de meios de comunicação social que possam comprometer a legitimidade das eleições e a liberdade do voto.

O Ministério Público Eleitoral tem uma função constitucional muito importante e deve ser procurado, podendo apresentar denúncias e as próprias ações, que também podem ser iniciadas pelos partidos, coligações e candidaturas.

Código Eleitoral - *Lei nº 4.737/1965*

O Código Eleitoral, *Lei nº 4.737*, é o principal marco legal para combater violência política e desinformação na Internet durante as eleições, prevendo em seus arts. 222 e 242 que a propaganda não pode ser falsa ou sensacionalista. Vale citar que o *Código Eleitoral* também determina sanções para o crime de injúria na propaganda eleitoral (art. 326) e denunciação caluniosa (326-A) com finalidade eleitoral.

Crimes eleitorais relacionados

Art. 323. Divulgar, na propaganda, fatos que sabe inverídicos, em relação a partidos ou candidatos e capazes de exercerem influência perante o eleitorado

Art. 326. Injuriar alguém, na propaganda eleitoral, ou visando a fins de propaganda, ofendendo-lhe a dignidade ou o decoro:

Art. 326-A. Dar causa à instauração de investigação policial, de processo judicial, de investigação administrativa, de inquérito civil ou ação de improbidade administrativa, atribuindo a alguém a prática de crime ou ato infracional de que o sabe inocente, com finalidade eleitoral:

§ 3º Incorrerá nas mesmas penas deste artigo quem, comprovadamente ciente da inocência do denunciado e com finalidade eleitoral, divulga ou propala, por qualquer meio ou forma, o ato ou fato que lhe foi falsamente atribuído.

Lei Eleitoral - Lei n. 9.504/1997

A chamada ***Lei Eleitoral*** também é um mecanismo importante de defesa de direitos, pois em seu art. 57 proíbe condutas que promovam a propaganda eleitoral irregular na Internet, como falsear identidade, atribuir indevidamente autoria a terceiros, alterar conteúdo de outrem, e tenta proteger também a privacidade, dispondo sobre um **dever de descadastramento** (art.57-G) de mensagens eletrônicas enviadas (spam político) a pedido do destinatário. Prevê multa para quem violar as disposições:

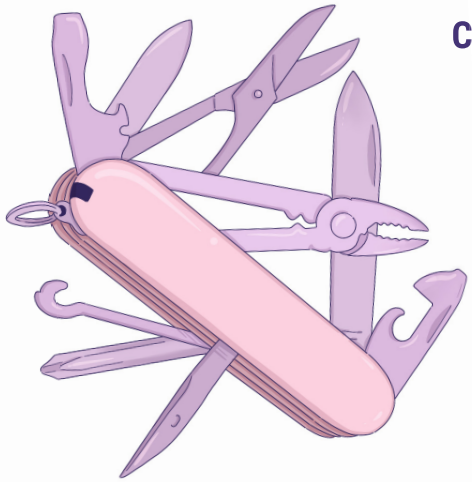
> § 2o A violação do disposto neste artigo sujeita o responsável pela divulgação da propaganda e, quando comprovado seu prévio conhecimento, o beneficiário à multa no valor de R$ 5.000,00 (cinco mil reais) a R$ 30.000,00 (trinta mil reais).

Resolução nº 23.610/2019

A edição da ***Resolução nº 23.610*** pelo TSE (2019) foi um passo importante no sentido de atualizar algumas previsões da Lei das Eleições, regulamentando a Propaganda Eleitoral nas eleições de 2020. Tal resolução contém disposições que proíbem propaganda discriminatória ou que calunie, difame ou injurie qualquer pessoa ou órgão (art.22), prevendo também a remoção de conteúdo por ordem judicial no caso de violações às regras eleitorais ou ofensas a direitos de pessoas que participem do processo eleitoral (art.38). Proíbe ainda o uso de perfis falsos e robôs para propaganda eleitoral e traz punições para casos de divulgação de informações inverídicas (art. 23). Finalmente, a ***Resolução nº 23.610*** trouxe uma maneira de interpretar a Lei das Eleições de forma mais protetiva em relação aos dados dos usuários da Internet, incorporando menções à Lei Geral de Proteção de Dados.

Legislação Penal

A Legislação penal nos traz algumas possibilidades para denunciar cada caso de violência: a denúncia pode ser feita de forma anônima e online, e ao ser recebida será encaminhada ao Ministério Público, que decidirá sobre a investigação. Como veremos nos quadros abaixo, as condutas podem ser enquadradas como crimes contra a honra - calúnia, difamação ou injúria; como um dos crimes contra a paz pública - quando ocorre incitação ao crime ou apologia; ou ainda como crime contra a liberdade pessoal.



Código Penal de 1940

Nos casos de divulgação de desinformação, quando é disseminada notícia falsa sobre você, imputando uma conduta criminosa ou ofensiva, artigos cabíveis para denunciar são os art.138 e 139 de calúnia ou difamação:

Calúnia

Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como **crime**:

Pena - detenção, de seis meses a dois anos, e multa.

§ 1º - Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga.

§ 2º - É punível a calúnia contra os mortos.

Difamação

Art. 139 - Difamar alguém, imputando-lhe fato **ofensivo** à sua reputação: Pena - detenção, de três meses a um ano, e multa.

Nos casos de discurso de ódio direcionado a você, ofensas, xingamentos, agressões, as condutas podem estar descritas no art. 140, que trata sobre injúria, ou até mesmo no § 3º, que traz a **injúria racial** e ofensas com a utilização de elementos referentes a raça, cor, etnia, religião, origem, a condição de pessoa idosa ou com deficiência.

Injúria

Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:

Pena - detenção, de um a seis meses, ou multa.

Lei Antirracismo - Lei nº 7.716/1989

No caso do crime de racismo, a *Lei Antirracismo* prevê que *praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional* é crime **inafiançável e imprescritível,** e a pena é agravada se o ato se deu por intermédio dos meios de comunicação social ou publicação de qualquer natureza[11].

Em situações de ameaças ou intimidação, o art.147 pode ser trazido na notícia do crime cibernético:

Ameaça

Art. 147 - Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave:

Pena - detenção, de um a seis meses, ou multa.

Se alguém teve algum benefício econômico a partir do uso violento, enganador das redes sociais, é possível enquadrar a conduta no crime de estelionato. Ainda, se o discurso de ódio ou desinformação foi realizado a partir de uma conta falsa ou bot, induzindo o eleitor a erro, é o caso do crime de falsa identidade.

Estelionato

Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento.

Pena - reclusão, de um a cinco anos, e multa

Falsa identidade

Art. 307 - Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem.

Pena - detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave.

11 (art. 20, parágrafo segundo)

Quando o discurso de ódio envolver incitação ao crime ou apologia:

Incitação ao crime

Art. 286 - Incitar, publicamente, a prática de crime:

Pena - detenção, de três a seis meses, ou multa.

Apologia de crime ou criminoso

Art. 287 - Fazer, publicamente, apologia de fato criminoso ou de autor de crime: Pena - detenção, de três a seis meses, ou multa.

Lei das Contravenções Penais - Decreto-lei n. 3.688/1941

Outras condutas, menos graves, podem ser denunciadas a partir da **Lei das Contravenções Penais**, de competência dos Juizados Especiais Criminais, *como em casos de perseguição, "stalking" e outras ofensivas:*

Art. 41. Provocar alarma, anunciando desastre ou perigo inexistente, ou praticar qualquer ato capaz de produzir pânico ou tumulto:

Art. 42. Perturbar alguém, o trabalho ou o sossego alheios

Art. 65. Molestar alguém ou perturbar-lhe a tranquilidade, por acinte ou por motivo reprovável.

Combate à violência de gênero na Internet

Os artigos aqui mencionados do Código Penal passaram por alterações para abarcar especificamente a violência de gênero envolvendo tecnologias. A partir de uma necessidade que eclodiu com casos concretos, duas leis foram elaboradas sobre o tema:

Lei Carolina Dieckmann - Lei n. 12.737/2012

Lei Carolina Dieckmann (2012) dispõe sobre a invasão de dispositivo, incluiu o artigo 154-A no Código Penal, criminalizando a invasão de dispositivo móvel para obtenção, adulteração ou destruição de dados ou informações, sem autorização expressa ou tácita do titular do dispositivo.

Lei Lola - Lei n. 13.642/2018

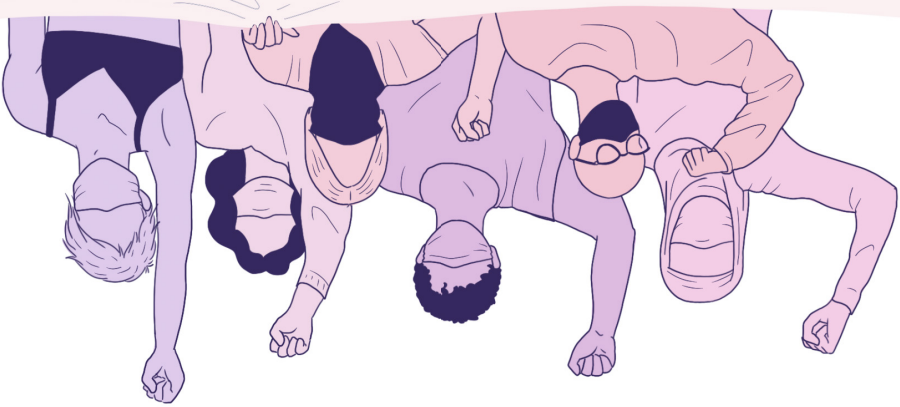
Lei Lola (2018) permite a investigação pela Polícia Federal de **discurso misógino na Internet,** ou seja, de conteúdo que propaga o ódio ou a aversão às mulheres.

Lei Maria da Penha - Lei nº 11340/2006

Ainda, as vítimas podem memorar sempre a **Lei Maria da Penha (Lei nº 11340/2006)**, principalmente após sua alteração, em 2018, que passou a considerar crime registro íntimo não consentido. No ambiente das redes sociais e dispositivos, sobretudo os artigos 5 e 7 da Lei Maria da Penha são relevantes, pois classificam **a violência psicológica** como um dos elementos possíveis para se pedir proteção e demandar inclusive medidas protetivas de afastamento.

Criminalização da LGBTfobia - STF ADO 26 e MI 4733

A decisão pela criminalização da LGBTfobia (2019) no julgamento do STF nas ações ***ADO 26 e MI 4733*** também oferece suporte para combater a violência de gênero na Internet, pois a Suprema Corte entendeu que a discriminação em razão da identidade de gênero no caso da LGBTfobia é análoga ao racismo até que o Congresso Nacional crie uma legislação específica. Portanto, é crime.



Analisando violências

Desinformação, discurso de ódio e ataque massivo - As denúncias podem ser feitas em todas as esferas possíveis e enquadradas como crimes contra a honra. O denunciante pode denunciar as práticas nas plataformas (importante guardar uma cópia da denúncia, se possível em print screen).

Na esfera penal, é importante o registro da ocorrência pela delegacia de polícia, pelo ***formulário eletrônico*** e o acompanhamento da denúncia no sentido de cientificar a autoridade policial do interesse na representação do ocorrido. Nos casos de crimes contra a honra, a ação será a penal privada, apresentada em juízo pelo próprio ofendido ou representante legal, por meio de um advogado. Nesta oportunidade, além da resposta penal, há a possibilidade de imputação de responsabilidade civil do autor da desinformação e do discurso de ódio por parte do juízo penal.

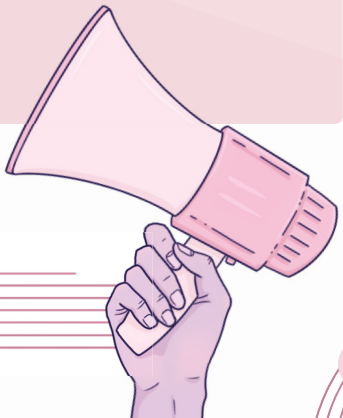
Na esfera cível, a pessoa signatária da violência pode requerer, por meio de ação de dano moral e material, ressarcimento de todo o dano ilícito causado, sendo possível também o requerimento de retirada do conteúdo produzido tanto na esfera online quanto a produção física do discurso de ódio.

Canais de denúncia e possibilidades de enfrentamento: respostas efetivas a ataques na Internet

Quando o discurso de ódio é realizado por parlamentares já eleitos, esbarra na imunidade parlamentar, podendo ser contestado internamente no Congresso Nacional, nas assembleias e câmaras municipais quanto ao decoro parlamentar, sendo cabível também o ajuizamento ações cíveis de indeniza-

ção e direito de resposta, a depender da gravidade do caso. Torna-se cada vez mais importante acompanhar os casos, no esforço de documentação, compreensão do problema e categorização de formas de violência. Algumas iniciativas poderão tangenciar neste esforço de coleta de denúncias com as dificuldades de lidar com a manifestação destas formas de violência online no contexto político:

- **Câmara dos Deputados:** já disponibilizou seu canal de denúncias para receber casos de violência política de gênero no ***Fale Conosco da Casa***.
- **SaferNet:** ***em parceria com o MPF,*** a partir das denúncias que recebe, pretende oferecer elementos para a investigação de crimes eleitorais praticados a partir da web.
- **Clique 180:** aplicativo de combate à violência contra a mulher, para o caso de ter existido relação afetiva entre agressor e vítima.
- ***TretAqui.org*:** coletará denúncias de links com disseminação de conteúdos de ódio ou discriminatórios proferidos por campanhas e contra campanhas nas eleições.
- **Aliança Nacional LGBTI+**: está montando um grupo de advogados para receber e orientar denúncias de ataques LGBTfóbicos contra candidaturas LGBTQIA+.



Redes de apoio

Normalmente, toda candidatura já nasce de uma rede de apoio com base em valores comuns. Em caso de ataque, lembrem-se, vocês não estão sós. Como equipe da campanha, ativem essa rede de apoio, seja para denunciar ataques ou para promover contra-discurso. Mas, ao fazer denúncias, lembrem-se sempre que, ao compartilhar conteúdo ofensivo, pela lógica dos algoritmos das redes sociais, vocês também estão dando visibilidade para o agressor. O ideal é que a campanha seja estratégica também para pedir apoio dessa rede. Denúncias coordenadas nos sistemas internos das plataformas tendem a surtir mais resultado do que uma denúncia isolada, mas se quiserem envergonhar publicamente o ofensor, a sugestão é não compartilhar o post ou o perfil. Lembrem-se que muitos usam do ódio e da desinformação como marketing político para ganhar seguidores.

FORTALECIMENTO DO ESPAÇO DEMOCRÁTICO DA INTERNET

Esta cartilha trouxe algumas ferramentas práticas para potencializar a capacidade cidadã de desarticular campanhas de desinformação e discurso de ódio na Internet e para terem seus dados pessoais protegidos, em uma investida para informar toda a sociedade sobre seus direitos, sobre ferramentas para atuar com segurança nas redes e para incentivar candidaturas, sobretudo de grupos minorizados, na busca de uma maior representatividade de vozes na democracia, a partir da presença de mulheres, negras, indígenas, LGBTQIA+ e de outros grupos que, apesar de numerosos na população, ainda representam uma pequena parcela dos nossos representantes políticos. Acreditamos ser possível construir candidaturas fortes e conquistar eleitores através das plataformas com segurança digital, cuidado e responsabilidade. Consolidar os mecanismos de denúncia e proteção existentes, além de construir redes e laços de solidariedade virtuais para a transformação social são um caminho para que a e-democracia seja um espaço onde todos e todas possamos nos sentir seguros/as e representados/as.

REFERÊNCIAS DA CARTILHA

Adilson, José Moreira. *O que é discriminação?* Ed. Letramento, 2017.

Anthony, Tom, "Zoom Security Exploit – Cracking private meeting passwords", 2020. Disponível em: https://www.tomanthony.co.uk/blog/zoom-security-exploit--crack-private-meeting-passwords/.

CFEMEA - Centro Feminista de Estudos e Assessoria, *Guia Prática de Estratégias e Táticas para a Segurança Digital Feminista*, 2017. Disponível em: https://feminismo.org.br/guia/guia-pratica-seguranca-cfemea.pdf.

Coalizão Direitos na Rede, *A importância social e econômica da Criptografia*, 2020. Disponível em: http://cartilhacriptografia.direitosnarede.org.br/cartilhacriptografia.pdf.

Coding Rights, *Dados e Eleições 2018,* 2018. Disponível em: https://www.codingrights.org/dataelections.

Coding Rights, *Visibilidade Sapatão nas Redes,* 2020. Disponível em: https://codingrights.org/docs/visibilidade_sapatao.pdf.

Coding Rights; InternetLab, *Violências de gênero na Internet: diagnóstico, soluções e desafios*, 2017. Disponível em: https://www.codingrights.org/wp-content/uploads/2017/11/Relatorio_ViolenciaGenero_v061.pdf. Mapa dinâmico de Tipologias de Violência de Gênero Online disponível em: https://graphcommons.com/graphs/18d1331e-0021-4c1f-9a80-55b637b7c5dc__2a3d06dc.

Cox, Joseph, "Zoom iOS App Sends Data to Facebook Even if You Don't Have a Facebook Account", Vice - Motherboard, 2020. Disponível em: https://www.vice.com/en_us/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont--have-a-facebook-account.

Doms, Caroline, "Como funciona o StreamYard? Saiba tudo sobre plataforma para fazer lives", *TechTudo,* 2020. Disponível em: https://www.techtudo.com.br/

listas/2020/07/como-funciona-o-streamyard-saiba-tudo-sobre-plataforma-para-fazer-lives.ghtml.

Gendersec.tacticaltech.org wiki, "Zen y el arte de que la tecnología trabaje para ti", 2015. Disponível em: https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual/es#Creando_y_gestionando_identidades_en_l.C3.ADnea

Gênero e Número, *Violência contra LGBT+ nos contextos eleitoral e pós-eleitoral,* 2019. Disponível em: http://violencialgbt.com.br/em-pesquisa-sobre-violencia-contra-lgbt-no-contexto-politico-eleitoral-mais-de-50-dizem-ter-sofrido-pelo-menos-uma-agressao/.

Hiperderecho, *Conocer para resistir: violencia de género en línea en Perú*, 2018.

InternetLab, *Santinhos, memes e correntes: um estudo sobre spam político no WhatsApp,* 2019. Disponível em: http://www.internetlab.org.br/pt/informacao-e-politica/santinhos-memes-e-correntes-um-estudo-sobre-spams-nas-eleicoes/.

Instituto Alziras, *Perfil das Prefeitas no Brasil: mandato 2017-2020", "Eleitas: mulheres na política,* 2018. Disponível em: http://alziras.org.br/projetos#PrefeitasBrasileiras.

Instituto Update, *Eleitas: mulheres na política*, 2020.

Lee, Micah; Grauer, Yael, "Apesar da propaganda, não há criptografia de ponta a ponta nas reuniões feitas pelo Zoom", The Intercept_Brasil, 2020. Disponível em: https://theintercept.com/2020/04/06/zoom-reunioes-criptografia-coronavirus/.

Luchadoras, *Violencia política a través de las tecnologías en México*, 2018.

ONU Mujeres, *Historias de violencia hacia las mujeres en la política en América Latina,* 2019.

Peña, Paz; Varon, Joana, *Consentimento: nossos corpos como dados: contribuições das teorias feministas para o debate de proteção de dados,* 2019. Disponível em: https://www.codingrights.org/relatorio-consentimento-nossos-corpos-como-dados--contribuicoes-das-teorias-feministas-para-reforcar-a-protecao-de-dados/.

Tactical Tech, *Personal Data: Political Persuasion*, 2019. Disponível em: https://cdn.

ttc.io/s/tacticaltech.org/methods_guidebook_A4_spread_web_Ed2.pdf.

Teixeira, Lucas, "*Abre-te Sésamo: as senhas da nossa vida digital*", Medium Coding Rights, 2017. Disponível em: https://medium.com/codingrights/abre-te-s%C3%A-9samo-as-senhas-da-nossa-vida-digital-469a8772723a.

União Interparlamentar, *Sexism, harassment and violence against women in parliaments in Europe,* 2018.

Velasco, Ariane, "Dois WhatsApp no mesmo celular: como ter duas contas no Android", Canaltech, 2020. Disponível em: https://canaltech.com.br/apps/saiba-como-ter-duas-contas-do-whatsapp-em-um-mesmo-celular/.

LINKS ÚTEIS

';--have i been pwned?: https://haveibeenpwned.com/

#SeguridadDigital: Que Mercúrio retrógrado no afecte tus comunicaciones digitales!: https://fortuna.segudigital.org/es

AccessNow Helpline - Linha de Ajuda em Segurança Digital: https://www.accessnow.org/help-pt/?ignorelocale

Agência Lupa: https://piaui.folha.uol.com.br/lupa/

Aos Fatos: https://www.aosfatos.org/fatima/

Bot Sentinel: https://botsentinel.com

Ciberseguras: https://ciberseguras.org/materiales/

Citizen Lab - Security Planner: https://securityplanner.org/

Coding Rights - Safermanas: dicas de segurança digital em gifs!: https://www.codingrights.org/safermanas-dicas-de-seguranca-digital-em-gifs/

Coding Rights - Safermanas #1 Apps de Chat: https://www.codingrights.org/wp--content/uploads/2018/05/01_safermanas_pt.gif

Deseat.me: https://www.deseat.me/

Frontline Defenders - Digital Security Resources: https://www.frontlinedefenders.org/en/digital-security-resources

G1 - Fato ou Fake: https://g1.globo.com/fato-ou-fake/

Guia de Autodefesa Digital: https://guia.autodefesa.org/

Kit De Primeiros Socorros Digitais: https://digitalfirstaid.org/pt/

Modo a Prueba de Riesgos: https://modeladoriesgos.asuntosdelsur.org/

Pornografia sem consentimento: Cinco recomendações para denunciar e resistir

com a sua publicação: https://acoso.online/br/

Presidência da República, Lei n. 12.965/2015 - Marco Civil da Internet: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

Presidência da República, Lei n. 13.488/2017 - Reforma no ordenamento político-eleitoral: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Lei/L13488.htm

SaferNet - Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos: https://indicadores.safernet.org.br/index.html

Seja Monstra: identidades para nossa vida cotidiana: https://sejamonstra.net/

Sleeping Giants Brasil: https://twitter.com/slpng_giants_pt

Surveillance Self-Defence - Autodefesa contra Vigilância: Dicas, ferramentas e tutoriais para uma maior segurança nas comunicações online: https://ssd.eff.org/pt-br#index

Surveillance Self-Defence - Como evitar ataques de Pesca (Phishing): https://ssd.eff.org/pt-br/module/como-evitar-ataques-de-pesca-phishing

Surveillance Self-Defence - Como utilizar o KeePassXC: https://ssd.eff.org/pt-br/module/como-utilizar-o-keepassxc

Tactical Tech - Holistic Security: https://holistic-security.tacticaltech.org/introduction.html

TretAqui.org - Discurso de Ódio nas Eleições não Dá: https://www.tretaqui.org/

TSE - Tribunal Superior Eleitoral, Estatísticas do Eleitorado: http://www.tse.jus.br/eleitor/estatisticas-de-eleitorado

TSE - Tribunal Superior Eleitoral, Divulgação de Candidaturas e Contas Eleitorais: http://divulgacandcontas.tse.jus.br/

TSE - Tribunal Superior Eleitoral, Financiamento Coletivo: http://www.tse.jus.br/eleicoes/eleicoes-2020/prestacao-de-contas/financiamento-coletivo

TSE - Tribunal Superior Eleitoral, Sistema de Prestação de Contas Eleitorais (SPCE): http://www.tse.jus.br/eleicoes/eleicoes-2020/prestacao-de-contas/sistema-de-prestacao-de-contas-eleitorais-spce

VPN Rise Up: https://riseup.net/en/vpn

COALIZÃO
DIREITOS
NA REDE